The Third International PKI Survey

OASIS PKI Technical Committee (Lower Costs Subcommittee)

Add here Intro & objectives

The questionnaire consists of fours parts organised in separate work sheets. Part A captures demographic details for each respondent; Part B gathers quantitative data on various topics, many in common with previous surveys; Part C asks for qualitative feedback and opinions. Part D goes over two worksheets, gathering data on a single PKI project as nominated by the respondent. The first sheet for Part D captures the characteristics of the project, and asks you to show how various elements were implemented. The second sheet then asks you to specify the costs expended on each element; cost data can be provided in relative terms (where no actual dollar figures need be disclosed) or in absolute values (if you are comfortable sharing such data).

Add here a privacy statement, and instructions

PART A: DEMOGRAPHIC DATA

Your name

Organisation

Position / Job Title (please tick only one)

- IT related security □
- IT Staff □
- IT Management □
- Non-IT management □
- Product developer □
- Researcher □
- Software developer □
- Auditor □
- Lawyer □
- Other (please describe) □

How many years experience do you have in Information Security or Privacy?

What experience do you have in PKI? Please indicate your highest level of involvement

- Read about PKI □
- Considered using PKI □
- Used PKI □
- Helped deploy PKI □
- Developed PKI related software □

What is your organisation's principal business sector? Please tick only one

Government □
Healthcard □
Education □
Finance □
Manufacturing (computer related) □
Manufacturing (non computer) □
Other Services (please describe) □ □
Other (please describe) □ □

What is your organisation's size, with regard to number of employees?

1 to 99 □
100 to 499 □
500 to 999 □
1,000 to 9,999 □
Over 10,000 □

Which country are you based in? □

Please ignore any countries you might work in temporailly, unless a posting has lasted substantially the entire past 6 months.

Contact details

Would you be willing to participate in the OASIS PKI Survey again? □

If so, please provide your e-mail address for follow up.

Note, in accordance with our Privacy Policy, your details will only be used in order to follow you up for future surveys. All survey data is strictly de-identified before analysis and publication. No contact details are forwarded to any other organisation for any other prupose.

□

The Third International PKI Survey

OASIS PKI Technical Committee (Lower Costs Subcommittee)

PART B: QUANTITATIVE & TREND DATA

We are particularly interested in examining trends in PKI usage and experience over time. The questions in this section are matched to Surveys one and two, and allow us to extract trend data.

GENERAL INSTRUCTIONS

In many of the questions in this section, we ask that you allocate points to each item in a list of items or issues, to reflect how you rank them in importance. We suggest that you allocate a total of 10 points, any way you like. If one item happens to matter greatly to you, while none of the others matter at all, you can allocate all 10 points to that item. On the other hand, if five items all matter about the same, you could give them each two points. Feel free to use up more than ten points if that helps you think more clearly; we will normalise the total to ten when processing the data.

Have you participated in a past OASIS PKI Survey? □ *Y/N*

Please allocate a total of 10 (or more) points across the following 15 obstacles, to reflect their importance to you

Costs too high	□
Enrolment too complicated	□
Hard to get started – too complex	□
Hard for IT to maintain	□
Hard to use for end users	□
Insufficient Need	□
Lack of management support	□
PKI poorly understood	□
Poor Interoperability	□
Revocation hard	□
Smartcard problems	□
Software Applications don’t support PKI	□
Standards problems	□
Too much focus on Technology, not enough on Need	□
Too much legal work required	□

Please allocate a total of 10 (or more) points across the following 10 potential improvements to application software, to reflect your need for each of them.

Code Signing	□
Document Signing	□
Electronic Commerce	□
Single Sign On	□
Secure Email	□
Secure RPC	□
Secure Wireless	□
Virtual Private Network	□
Web Server Security	□
Web Services Security	□

Looking at *Document Signing* in more detail, how do you rate these sub-categories?

	Critical	Important	Imaterial
Signing documents before distribution (for integrity & origin)	□	□	□
Signing electronic forms	□	□	□
Signing contracts	□	□	□

Please allocate a total of 10 (or more) points across the following nine cost items to reflect which are the most problematic

Cross-Certification	□
End-user support	□
Initial certificate issuance	□
Initial system design	□
Non-technical setup costs (e.g. legal & CPS)	□
On-going operations	□
Secure facilities	□
Smartcards and Readers	□
Software acquisition	□
Software integration	□
Support Contracts	□
Training	□
Other Costs (please name)	□

Looking in more detail at the issue of *PKI being poorly understood* , please allocate a total of 10 (or more) points across the following six types of player to indicate where greater understanding is needed.

IT Management □

IT Staff □

Senior Management □

Users □

Vendors □

Other (please name) □

Looking in more detail at the issue of *Poor interoperability* , please allocate a total of 10 (or more) points across the following eight topics to indicate where you believe the most serious interoperability problems arise.

Certificate issuance □

Certificate revocation □

Cross-certification □

Path validation □

Protocols that use PKI (such as SSL or S/MIME) □

Smartcards □

Unusual certificate contents □

Other (please name) □

The Third International PKI Survey

OASIS PKI Technical Committee (Lower Costs Subcommittee)

PART C: YOUR COMMENTS and QUALITATIVE FEEDBACK

GENERAL INSTRUCTIONS

Most of the questions in this Part have free text answers. Feel free to insert and use more space for your answers if you need it.

Previous OASIS PKI surveys have identified the following three major "themes" relating to cost. Please comment on how any or all of these affect your use of (or views about) PKI?

Promoting specific standards that avoid the need for customization

Encouraging free PKI software and free CAs for low-assurance applications

Encouraging free PKI software and free CAs for low-assurance applications

Can you comment on any inadequacies that concern you in software application support for PKI (see also Q Bnnn)?

Can you comment on how organisations like OASIS could assist with improving application support?

Can you comment on how organisations like OASIS could assist with improving the understanding of PKI?

Are you aware of the PKI resources of OASIS at www.pkiforum.org/resources, and if so, have they been of use to you?

What has been your dominant or most valuable source of PKI information?

Please feel free to provide any further comments on PKI

The Third International PKI Survey

OASIS PKI Technical Committee (Lower Costs Subcommittee)

OASIS PKI

PART D: IMPLEMENTATION CASES

In this section we will ask you about a particular PKI project with which you have direct experience. We would like you to break down costs in relation to the "Digital Certificate Supply Chain". First you describe how each element of the supply chain was implemented; then you look at what proportion of total costs were expended on each element.

If you would like to tell us about more than one implementation, please use another worksheet

Project details

Project name (for easy reference)	□	The name used here need not be "official".
Your role in project	□	e.g. Project Manager, Consultant, Engineer, Business Sponsor

Principal underlying security function of the PKI-enabled app **(please tick one)**

- Transport security (e.f. IPSEC) □
- Authentication (including Single Sign On or Access Control) □
- Document Signing (or "non repudiation") □
- Other (please name) □

Principal business function of the PKI-enabled app **(please tick one)**

- Secure forms □
- Secure e-mail □
- Office automation □
- Work flow (including ERP) □
- Procurement, trading □
- Embedded software □

Software technologies and platforms involved (tick as many as apply)

MS Windows NT or 2000 □

MS Windows XP or 2003 □

MS Windows Longhorn □

UNIX/Linux □

Mac OS X □

Mac pre OS X □

Special purpose OS (e.g. embedded control) □

Web Services □

SSL/TLS □

XMLencryption □

XMLsignatures □

XPATH □

Other XML variants (please name) □

□

Principal business sector (please tick only one)

Government -- service delivery to citizens □

Government -- internal, administration etc □

Banking & Finance -- retail □

Banking & Finance -- institutional, merchant, funds management □

Healthcare □

Education □

Customs & international trade □

□

Other (please describe) □

Project approval and initiation

Did you quantify ROI in order to justify the PKI project in question? □ *Y/N*

If not, why not? □

Was a positive ROI explicitly required by management before approving? □ *Y/N*

Or was PKI treated as “strategic”, not in need of quantitative ROI? □ *Y/N*

Project outcomes

What is the current status of the PKI project? Please tick only one.

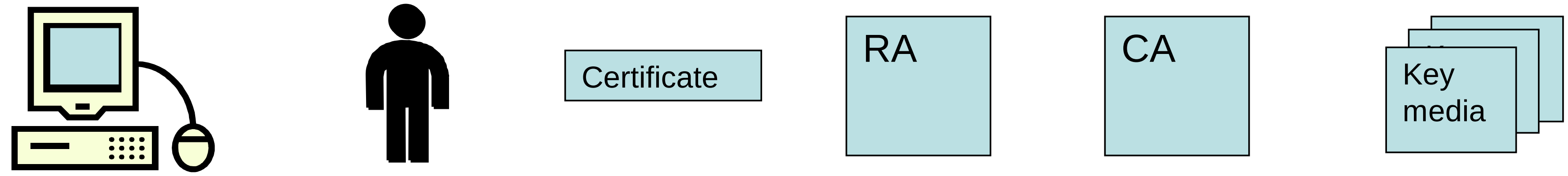
- Design and/or development still underway □
- Advanced stages of testing or beta deployment □
- Operational □
- Cancelled after going live □
- Cancelled before going live □
- Undergoing major re-work after going live □
- Other (please describe) □ □

How would you describe the outcome of the PKI project? Please tick only one.

- Very satisfactory; objectives and expectations met or exceeded □
- Satisfactory; most objectives met □
- Unsatisfactory; few objectives met □
- Unknown; too early to tell □
- Other (please describe) □ □

Modes of implementation

According to the Digital Certificate Supply Chain model, there are up to six major elements in any PKI implementation. Each of these can be implemented in various ways. Below we sketch out the supply chain and list some of the most common modes of implementation foir each element. Please tick which apply to your project and comment on any special local issues.



Certificate

RA

CA

Key media

Application related

Fat client? □

Or Thin Client? □

Off the shelf? □

Or developed in-house? □

Major customisation? □

User related

Gen purpose certs? □

Or app-specific? □

Certificate related

Do you pay per cert? □

Pay for OCSP check? □

Pay for X.500 access? □

RA related

Third party RA? □

Or enterprise RA? □

CA related

Third party CA? □

Enterprise CA, in-house? □

Enterprise CA, hosted? □

Key media related

Soft certificates? □

Roaming soft certs? □

USB keys? □

Smartcards? □

Other? □

Other implementation details

Was the project subject to security or management standards? Please name □ *Y/N* □

If so, was your project formally audited according to those standards? □ *Y/N*

"Post Project Review"

Were all of the PKI elements clear to you at the start of project? □ *Y/N*

Did any particular elements over time? How? □ *Y/N*

Which PKI elements were most costly in absolute terms?

Which elements were most difficult to control in terms of costs?

Which elements tended to over run expected costs?

Which if any elements come in under budget?

What specifically did you do to control costs during deployment?

Which if any costs seem to you especially unreasonable?

If you were to start again, what would you do differently?

Based on your experience, how do you think the following costs may change in future **in your business?**

Please feel free to add comments at the right

	Worsen	Same	Improve	
Economies of scale with more users on board				
Technology evolution				
Competition amongst CAs				
Simpler (or less) application integration				
Lower user support overheads				
Other (1)				
Other (2)				
Other (3)				

PART D CONTINUED: IMPLEMENTATION CASES

This section carries on from the Implementation Modes for a given PKI project. If you have nominated the ways in which each element of your PKI project was implemented, now we would like you to describe the costs associated with each element. There are two ways you can choose to describe costs: either (1) nominate actual dollar amounts, if you are comportable and allowed to do so, or (2) allocate a total of 10 (or more) points to each alternative in each section, to reflect the proportion of your expenditure.

	Fixed set-up Costs	**Variable set-up Costs**	**Fixed Annual Costs**	**Variable Annual Costs**
1. Application related costs				
Fat Client	Developer training □			
	Recruiting □			
	Contractor fees □			
	PKI related design & devt □		Code maintenance □	
	PKI systems integration □			
	PKI toolkit licenses □		PKI toolkit support fees □	PKI toolkit support fees □
	Other third party SW lic's □		Other third party support □	Other third party support □
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □
Thin client	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □

	Fixed set-up Costs	Variable set-up Costs	Fixed Annual Costs	Variable Annual Costs
2. User related costs				
Gen Purp ID Certs	Marketing campaign □	User training □	Help desk □	Help desk □
		Educational materials □		
		Present to 3rd party RA □		Present to RA to renew □
		Cost of Id documents □		Revocations for key comp □
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □
	□	□	□	□
App Specific Certs				Revocations for key comp □
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □
	□	□	□	□
3. Certificates				Issuance/Renewal fee □
				Revocation charges □
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □
	□	□	□	□

	Fixed set-up Costs	Variable set-up Costs	Fixed Annual Costs	Variable Annual Costs
4. RA				
Gen Purp ID Certs				Liability cover □
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □
Enterprise Certs	RA software licence □		RA software support □	Liability cover □
	RA hardware □		RA hardware support □	
	RA HSM □		RA HSM support □	
	RA facilities □		RA compliance audit □	
	RA operator training □			
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □

	Fixed set-up Costs	Variable set-up Costs	Fixed Annual Costs	Variable Annual Costs
5. CA				
Hosted externally	Establishment charges □			Liability cover □
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □
In-house	CA software licence □		CA software support □	Liability cover □
	CA hardware □		CA hardware support □	
	CA HSM □		CA HSM support □	
	CA facilities & security □		Facility management □	
	CP/CPS development □		Facility security fees □	
	Ops documentation devt. □		Facility power & services □	
	Legal review & signoff □		CA audit □	
	CA operator training □			
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □

	Fixed set-up Costs	**Variable set-up Costs**	**Fixed Annual Costs**	**Variable Annual Costs**
6. Key Media				
Soft Certs				
Roaming soft certs	Software licence □			Roaming S/W support fee □
				Help Desk increment □
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □
	□	□	□	□
USB Keys		USB keys □		Replacements □
				Help Desk increment □
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □
	□	□	□	□
Smartcards	Custom artwork □	Cards □		Replacements □
	Custom personalisation □	Readers □		Reader support fees □
				Help Desk increment □
	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □	OTHER (describe) □
	□	□	□	□