Textual Comments from August 2003 Follow-up Survey on Obstacles to PKI Deployment and Usage

FOR INTERNAL USE ONLY

An Internal Document of the OASIS Public Key Infrastructure (PKI) Technical Committee (TC)

Author: Steve Hanna (Sun Microsystems, Inc.)

Date: September 23, 2003

Version: 0.1

DRAFT

Table Of Contents

Appendix A. Comments on How Application Support for PKI is Insufficient

The Follow-up Survey asked for comments on how application support for PKI is insufficient. The full text of these comments is included here. To preserve the privacy of the survey respondents, these comments should not be distributed beyond the PKI TC. However, they are summarized in the analysis of the survey.

The problem is more one of degree of consistent support...many of these applications do support PKI, sort of. They just don't do it in a consistent way. For example, when confronted with an extension flagged critical, three different applications may react differently if they cannot handle it....The standards are somewhat fuzzy to start with (as in open to interpretation) and implementations are all over the map.
Integrated PKI support is virtually non-existent in SSO, Web Services, and e-commerce offerings.
sUPPORT IS INCONSISTANT. METHOD USED FOR SIGNING ONE DOCUMENT FORMAT MAY NOT BE RECOGNIZED OR ACCEPTED BY ANOTHER, OR THAY MAY BE INCOMPATIBLE.
Some support, but not enough. Specifically with Electronic Commerce, the full range of PKI (support for all extensions) is often required for high value transactions--it's just not there.
Most valuable applications can be made PKI enabled but at a high cost
Most of the applications in the market does not provide enough support for LDAP verification. This is an essential part of the entire PKI process, which should not be overlooked, esp in document signing, webserver security or other EC transaction. Interoperability in different email application is critical ie Lotus, outlook is critical as these are the most common email apps in the market. This will help to drive the need to use certs for secure email. Some single sign on products does very little in using certificates for authentication or even connecting to LDAP for verification of user. This could be better improved.
Support is insufficient in that major EC applications son't recognize the need for higher levels of easily implemented and managed security. EC has not taken off to the degree it should because organizations are not willing to conduct major business transactions in a risky environment...also, like EDI, it is too hard, complicated and requires one-to-one agreements (of the most part)
Insufficient due to lack of support for certificate extensions. I.e. ability to ask if some extension is present, and if it is, what does it say. Also, clients need work to address privacy problems.
Programs used for making standard docs types and for sending e-mails should offer uniform digital signature functionality, accepted world-wide by all major vendors. This significantly improve an interoperability and usability. At the present there are often big differences in standards implementation even among two version of the same program!!!
Document Signing. Most organisations use the MS Office suit that completely lacks support for PKI services. There are no alternatives that have PKI support either. Also I did an investigation for a Swedish governmental agency last year regarding PKI support in Document Management software. The result was a disaster, out of six possible systems available for the agency on the Swedish market only one (1) could be delivered with PKI support (additional integration work needed though). Note that the sales representative from four of the companies stated that their product had PKI support even though it later showed not to be so. Support for symmetric encryption of documents was one example of what they thought was PKI... Another problem not discussed in his survey is the encryption of documents inside a document management system. We have had several large customers asking us for help with finding a system with PKI-enabled encryption.
CP/CPS is requred but why? If there isn't, what's problem? Is HSM really needed? For what? If there isn't, what's problem? If people who really and simply want to use Document Signing ask you the question above, it's hard for me to make them understood.
Problem is interoperability. In one case we had to support certain VPN product, email-client, SSO-product and PKI-client (Entrust). It was difficult to find certificate profile, which worked with all of them. We wnated to use the one and the same certificate for all applications. One big issue

is applications directory usage. Applications use certificate subject-name to guess where the certificate is located in the directory and use that location to fetch extra attributes. Every application seems to have different logic. PKI-vendor has also decided for us, how we should use the PKI and we don't have enough flexibility. We can't design the architecture, directory and certificate profile freely, but need to follow PKI vendor "rules". It means that the solution will not be ideal for us. Most organizations have directory hierarchy set up already and PKI must adapt to customes directory.
All of the above have some PKI support. Several user facing applications have poor end-to-end integration to ease the need for users to have complex understandings of e.g. revocation. Most or all of the above need better integration across application vendor / PKI vendor. In particular, we have an Entrust PKI deployed with most employees registered. No software we have yet seen adequately and usably integrates that very strong infrastructure with practical end user applications such as encrypted / signed email and encrypted filesystems. Entrust itself offers poor quality user applications and plug-ins. Microsoft's operating system offers fairly strong features, but with poor integration to other PKI vendors' infrastructures.
Most critical is the lack of a standard way to support signatures in webapplications. WebService Security is lacking a standard method for activations signing of data, and handling of signed data. (Data, not documents)
Many Email Servers and Systems do not provide an easy, flexable, and standards based deployment for PKI enabled Email Services. As well, the Interoperability between Email systems make key exchange, centralized key sharing, and overall interoperability very difficult. PGP, Verisign SecureMail Certificates, Microsoft Exchange, IMAIL, and a myriad of other methods of securing email exist, but as there is no "standard" and centralized key exchange/bridging mechanism, repudiating a source email normally requires jumping through hoops. Or simply enable your enterprise to support "ALL" types of PKI... an impossible task.
Universal PKI support is insufficient and not uniform
The majority of the applications noted above do offer PKI support, but in the case of some of these applications (e.g. Single Sign-on, WSS, and VPN) PKI is only one of several security options which can be used. Obvious improvements would be to make the PKI option de facto or more attractive option to use. The issue with document signing is that there are competing signature formats (e.g. PKCS#7, XML Dig Sig, etc) and implementation considerations (e.g. client versus server implementation). Debates over which is the best or right format or approach are holding up PKI implementation in a space.
PKI support is insufficient. do now provide basic 'hooks' in their products which will support the addition of a PKI application. The main desktop and operating systems should, at this stage, include some basic and easy to use functions as a matter of course. These basic functions should include: 1. Key generation and certificate process workflow, 2. Signature functions built into Documents, email, internet etc. or to any object created on the computer 3. The ability to process and validate the signature attached to any object
VPN is not compatible with the latest version of Entrust PKI therefore stops us from moving along with the change of key length
transparent email interoperability
The high ranking items have PKI support but are very important and need the most focus for improvement. One of the issues with signing is long term verification capabilities. Not enough effort in digital notaries and storage of veification information to prove a document was legally signed 50 years previous.
Generally support exist in all categories marked. However, usage, especially "first time configuration", is much too complicated for the general "office user", and requires a rather good understanding of PKI to be used properly and effectively. In all cases support needs to be much more transparent.
SSO is only partially suported, on some platforms
Not completely lacking, but rather problems exist in areas like cert revocation checking, integration of document signing into business process flows (I can sign a document but how best to do that as part of a business process), and dealing with historically made digital signatures (how to be sure that a signature made today can be validated in ten years).
Most application types have only limited PKI support, or make it difficult to use without advanced PKI knowledge on the part of the user.

Secure E-mail in the business world might just be the PKI killer app. Applications need to be beefed up to better support digital certificates, but there needs to be a major improvement in key management and initial registration. How do you (in a secure, cost-effective, manageable, reasonable way) get keys to a new user (customer) for secure Internet communications?
The area that most software application lack is "validation" support and the ability to accept certificates from multiple issuers.
It is insufficient. There is no widely available technology or it is not well known
Secure e-mail should be automatic and trivial for any user, but for 99.9% of e-mail this is not the case. Document signing is only done in specialized cases. Secure "telnet" like applications would make VPN more useful (here under single sign on).
Use of PKI at network layer devices is proprietary if at all. Requires too many protocols (per vendor) and is difficult to centrally manage
Every application (E-mail clients, browsers, PDF clients, etc) use SEPARATE (their own certs) in their own way, in their own format, with their own logic of validation, with their own rules of processing extensions, etc.
Some PKI Support, but either turned off by default, hidden as an advanced feature or too hard to get enrolled and get started.
Most of the applications above claim to have some certificate interoperability, but do not fully integrate the functionality or provide a limited set of API's.
Most have some sort of PKI support. But it's not interoperable or standards-compliant.
Secure Wireless LAN is not developed to the point where security is guaranteed, in my viewpoint. While it appears to be a usable product, there are significant flaws that need to be addressed first before I would use or develop a system to support it.
I see email as the starting point and until Microsoft and PGP see compatibility out of the box it will be a minor application. If MS bought and packaged PGP in outlook or some clone of it I cant see wider acceptance of PKI. But when this happens (IF) the level of acceptance and awareness of PKI will be shuch that the general public will be educated enough to accept its use.
e-commerce apps need deep integration of PKI functions -- transaction signing, certification verification, renewal reminders, better GUI design.
Most have some, but lack of standards and internal combats to win market shares are reducing the possibility to grow rapid markets.
cross-company s/mime encryption is essentially impossible today. There is no real solution out there. x.500 is not the answer.
Some support is there. Especially encryption functionality (for confidentiality) is very poor in most applications (when assymetric encryption is used).
though some email applications do support PKI functions, lack of interoperability and insufficient support is a big problem.
MS Word - lack of bridge support MS Wireless Lan clinet only supports certs with specific profiles
Insufficient. EVERY email client should support S/MIME "out of the box" (and maybe in addition PGP). For this to be real, finding each recipient's cert MUST be straight forward. Document (text, Word, PDF, XML, html, ...) signing needs standard, interoperable and easy to use products. Some of the ones I've used would frustrate a smart technologist! PKI is a great SSO but needs a "re-verification" mechanism (it isn't hard - just needs to be standardized). E-commerce should use federated identity (e.g. SAML) but until then needs a way to understand authorization as well as authentication.
Many email clients still don't support S/MIME and those that do often do it poorly and in ways that make life hard for users.
Almost everything at my institution requires TWO signatures, not one.
Document security - no support Web server security can't be guaranteed and not always supported secure email - no triple wrapping capabilities for mailing lists and certificate path discovery not implemented
Secure WLan is still complicated to integrate pki components.
In all cases the PKI systems available are not scalable and put too much reliance on client side security
Currently the only digital signature "standard" is S/MIME, so sharing signed documents without everyone using the same client is not possible. Also, validation in a bridge environment (e.g.,

FBCA) is not currently supported.
I beleive security in general needs to be looked at real close when dealing with PKI. With this technology individuals are putting their reputation on the line.
There is some support, but there must open standards if PKI is going to be widely used and adopted.
PKI support is not well integrated. Too many key stores, confusing error messages, too many dialog boxes buried too deep, poorly thought out logic and placement of features, etc.
For many of the applications above, such as web server security, VPN and Single Sign-On, there are products available that, if properly implemented, will process certificate-based authentication adequately. These kinds of applications leverage a portal approach, where certificates can be validated and trust decisions can be made in a single place. What is currently lacking is digital signature support for desktop applications that people frequently use (word-processing documents, spreadsheets, etc.). The latest versions of Microsoft Office applications do a better of supporting digital signatures, but not in a transactionally meaningful way. That is, the signatures are buried in the security layer, rather than using a metaphor, such as a signature block in the document itself, that people are used to. Also, there needs to be support for multiple signatures per document, with the ability for a signature to lock out certain sections of the document.

Appendix B. Comments on What the PKI TC or Others Could Do to Help Improve Application Support for PKI

The Follow-up Survey asked for comments on what the PKI TC or others could do to help improve application support for PKI. The full text of these comments is included here. To preserve the privacy of the survey respondents, these comments should not be distributed beyond the PKI TC. However, they are summarized in the analysis of the survey.

Encourage consistent implementations....that is try to develop implementation guidelines and work with the vendor community to modify their products to adhere to these guidelines....this also would be a major boon to interoperability.
Strongly promote lightweight PKI solutions and, more importantly, attribute certificate mechanisms; in most applications, the latter are much more effective than having to integrate an identity certificate mechanism (let alone an X.509-based one) into the front- & back-end. They bring many other benefits as well in many contexts. Identity certificates are too heavy-weight for many applications.
WORK TOWARD NATIONAL PKI STANDARDS, INCLUDING VENDORS FOR WORD PROCESSING AND DOCUMENT FORMATS THAT ARE WIDELY USED.
Integration with tokens (smart cards) should be made easier.
Different applications developers have different approach in incorporation signing or verification API in their applications. This could lead to interoperability issue in future. Thus, I was wondering whether does it makes sense to come up with a recommended (mandatory would not be possible) best practice for developers to develop such API.
Find a way to a) ensure, relative to the risk of the transaction, its security, b) in a totally transparent environment that is c) scaleable. (One of the biggest issues with PKI is the publishing and availablity of the public keys...solve that problem and you will have a chance at scaleing...)
No.
Do you think PKI system cannot be simple? The first step of PKI system is hard. Step by step development process of PKI is needed.
Educate vendors that their PKI product will not be the center of the universe, but it must adapt to customer environment. PKI-applications must be configurable to different certificate profiles and directory configurations.
Standardize the bridge capabilities or help to create a commercial bridge authority, that can repudiate certificates from multiple sources... i.e. I sign my email with a PGP key, and forward it to you, where you use a Verisign Class 3 Cert. A central bridge authority is queried to see if my PGP is valid, and repudiates me to you... and vice/versa.
Sponsor activities to profile the use of PKI in specific applications. Approach major industry players and encourage those companies to participate in OASIS and its activities. Provide education programs on PKI and its benefits - but not just from the technical perspective -- instead show how it can be an enabling technology and how integrating it into specific application spaces can make those applications easier to use or more useful to the business world etc.
There are very few serious players in the PKI market. The main business/Desktop software providers e.g. Microsoft, AppleMac, Sun etc., should be strongly encouraged to bundle a set of basic PKI functions, for each of the main PKI providers, within their products.
Not really unless go can push the vendors to be more up to date with the PKI technology.
Get the message out that Identity management is the current killer applicaition for PKI.

There is more than enough justification for this approach to deploy PKI... the rest will follow. Long term CRL management issues needs to be addressed. Not much noise here because we have yet to reach any real threasholds but that day will come and we need to be prepared. Digital norarization and its impact on making documents stand up in a court of law.
help businesses understand the benefits of PKI over simple SSL which is cheap and broadly used but not as secure - they need to understand why pay more - what extra benefits does one get, which ultimately would likely lead them to an outsourcing decision but at least use it where the risk warrants it
No
Provide a single standard followed by all PKI Service Provides or PKI software for validations (signature/path validation.) CRL is not the long term solution for clients. This would improve interoperabilty, reduce time/cost, and usability.
XML, XML, XML...
Automated secure e-mail. The user can turn it on or off, but that's it. Anything else makes the user have to learn more than they need to.
work towards getting device credential enrollment and management standardized
Create the standard specification (templates) of the PKI client (its functionality), PKI APIs/methods for applications to use client's functions, PKI protocols between PKI client and CA Servers, and for CA servers (functionality) to be used by PKI vendors for implementation of the PKI system and by application developers to access/use PKI functions
improved application support will only occur if/when PKI is gaining wide use. While far from offering a mature product, Microsoft may be that catalyst to get application developers building certificate awareness in their products.
Ensure that there are clear specs for application developers and help organize interop testing.
Not at this time.
See above
foster deep integration and automation of embedded PKI; foster application/scheme-specific PKI, so that enrolment overheads were reduced and legal arrangements simplified
Educate the market on the inherit security of PKI, ease of use as well as market the global use of PKI today. In this a comparrison the legacy systems might be good.
slow down the PKIX organization. Look at how many random drafts are ongoing - how can vendors possibly keep up? who uses attribute certs? stop making the standards so darn complex - it is a barrier to entry for software developers.
Focus on user friendliness and cost reduction!
Help outline standards for cert profiles
MOST IMPORTANT OF ALL: every O/S must support the cert cache and/or smart card device and related security services. Until then, each application will have to invent it's own. Furthermore, the O/S API should be as standardized as possible. MS has done some good work here bu where is Sun, Apple, etc.? Also see 4b above, and: take the top 5 email clients in terms of numbers. Get some one or group to add S/MIME support and give it back to the vendor. Altruistic perhaps; I call it priming the pump. Also, where is the directory-of-directories support for looking up a cert based only on the email address of the holder??? Clearly one could design the email client to store any ID cert received for later use in replying but that won't always be enough. WRT signing, there are standard encapsulations for some things, e.g. XML-DSIG, but there needs to be a generalized encapsulation standard (if one doesn't exist) that is used by all products. Then there needs to be reference implementations, including a user interface usable by non-technical people. See Alma Whitten's work at UC Berkeley, School of Information Mgmt & Systems (SIMS) for some good work in this area.
Provide two signature support.
Provide a specification which, for example, a secure email client requires to support in

PKI to work. Once this standard is in place, PKI will be used
Concentrate on client side security ie. s/cards are way to difficult and expensive to deploy and manage and identity theft is too easy for software only protection systems
Solve the client interoperability and bridge validation problem.
Advocate open standards.
Get Microsoft (and Apple) to improve usability and security of PKI features!!! Get drivers for smart cards and tokens included in Windows and OS/X. Help the world settle on one key store per operating system.
Encourage software publishers to incorporate digital signature capabilities into their products. Build validation discovery capabilities into applications, and into browsers, as signature verification without certificate validation does little to address legal values such as non-repudiation. Also, there needs to be some “best practices” published somewhere that business mangers could use to help them make decisions on how to store, retrieve and archive digitally signed records. There is a lot of reluctance to deploy electronic, digitally signed applications, despite their obvious benefits, due to fear of failing to account for these records in a manner that would satisfy audit requirements.

Appendix C. Descriptions of Other Costs

The Follow-up Survey allowed respondents to enter descriptions of Other Costs. The full text of these descriptions is included here. To preserve the privacy of the survey respondents, these comments should not be distributed beyond the PKI TC. However, they are summarized in the analysis of the survey.

Organisational problems such as lack of competence, project management, internal political struggle etc
Insurance on Secured Transactions
24 x 7 requirements which necesitate high availability (eg 99.999%) significantly increase costs. Production system requires mirroring as does any disaster recovery facility
maintenance costs
good technical staff are expensive, dual sites if high reliability required
Very low competency on the field makes it neccessarry to educate the customer in great detail. this is the true cost driver, not the compoents that are actually cheaper than competitive tech. One driver is of course the radical changes needed in core sy
Setting up a secure Certfication Authority
per seat / cert cost for end users
Developing the associated enterprise directories...
Managing client side security

Appendix D. Comments on What the PKI TC or Others Could Do to Help Reduce PKI Costs

The Follow-up Survey asked for comments on what the PKI TC or others could do to help reduce PKI costs. The full text of these comments is included here. To preserve the privacy of the survey respondents, these comments should not be distributed beyond the PKI TC. However, they are summarized in the analysis of the survey.

Although a lot has been done, still user awareness is key for PKI success.
The main thing would be how to help to drive the need for PKI. Once the user database increaases, the amount of ROI would subsequently be higher.
Standards - implemented in all vendor products - would reduce the costs, simplify the process and dramatically reduce the learning curve...but they would need some sort of certification as well to assure the markets that they are "standard"
No
Issuing free certificates and offering free certificate validation server such as an OCSP responder.
Provide the centralized service, at a per use cost... i.e. a tick fee, for each repudiation, it costs .10
Education programs targeted at businesses and consumer may help reduce costs associated with Training and end-user support since the technology will be more familar to people. Improved interoperability should reduce costs associated with the initial design and set-up of the system.
Not sure anything can be done. Secure facilities is a requirement because of support for medium assurance levels. Software cost is very high. Products like Entrust costing between $100 and $200 for a single license and that is before you talk about hardware, facilities, design, legal and other things. This is totally unreasonable.
support/promote consolidated/outsourced models as the way to go to drive up usage and down unit costs. Vendor license costs (certs) are still expensive, CA software itself is not, therefore increased usage can also be expensive unless buying volume up front.
No
Better standards and implementation tools would be advantageous - it seems everything you do in the PKI world is done from scratch as if no one else had ever done the same thing...
Bring the price of CA’s down, reduce the cost to have a ROOT authoirty sigh a sub.
At the very least: Eliminate the price per certificate model and adjust the pricing into the back-end management costs. Some certificates are more expensive if they are multi-use certs. That seems to be a bit like fleecing to me.
Promote smart card standards to reduce those prices. Encourage the development of free PKI software and free CAs for low assurance applications.
Develop a cost sharing, per use model that would allow multiple application connectivity for common PKI services.
Few people seem able to imagine scheme-based PKI, where certificates are issued to members for specific applications, under existing rules (be they professional association rules, employment rules, banking customer rules etc.) The greatest cost of PKI is legals, contracts, and end user training, all of which disappear under scheme based PKI. Another big cost aspect -- software design -- would be simpler if people could take advantage of scheme-specific PKI, and cease worrying about cross certification, public PKI, liability in open PKI etc etc.
In Sweden it is more important to create a different business model where costs should be kept low, similar to an annual subscription. This lowers the threshold for all involved which will ramp up the number of users faster and over time even generate more revenue.
Educate the markets and profile the ROI and TCO of a large scale corporate PKI as well as benefits for small/medium sized corporations
reduce the complexity to PKI deployment. the standards are so broad they mandate complexity to end users which is where the support costs are so high
Focus on interoperable use of certificates. Prevent users from obtaining a ’key chain’ of

certificates.
I believe that there needs to be a centralised, highly secure Certification authority (similar to a national passport office) acting as a service to anyone who needs it. This can act in concert with a multitude of Registration Authorities. Ideally any individual would have a single PKI identity.
provide a buying club for outsourced certs that would make it attractive for smaller institutions
This is actually a comment: The issue of cost is not absolute - what is importand is the cost/benefit ratio. Our management has yet to see a favorable cost/benefit ratio, mainly because of the factors I've identified above. Vendors of PKI services are beginning to see the light and make managed PKI based on "seats" instead of "certs." But the cost of the cert is minor compared to the rest of the required deployment.
Put massive pressure on certificate vendors; arrange higher education or other large group discounts for purchasing USB-certificate devices; provide cross certifying or bridged root authorities.
eliminate smart card and readers and replace with soft certs or usb tokens
Focus on scalability, no good having a you beaut key management infrastructure that cannot be deployed to the largest possible community of users. PKI is dying as mass deployment is never considered by the vendors.
I think if there was a common standard throughout industry for cards, software, and hardware this would assist in keeping cost down.
Help consolidate CA options to a couple of commercial packages, one high quality open source option, and several outsourcing providers.
Outsourcing should be considered to help reduce PKI costs. Outsourcing eliminates the need to hire and retain specialized staff, and allows organizations to take advantage of the economies of scale offered by full-time PKI providers. For those contemplating the formulation of a certificate policy of the first time, it is suggested that these organizations look closely at the Federal government

Appendix E. Descriptions of Other Parties who Need PKI Understanding

The Follow-up Survey allowed respondents to enter descriptions of Other Parties who Need PKI Understanding. The full text of these descriptions is included here. To preserve the privacy of the survey respondents, these comments should not be distributed beyond the PKI TC. However, they are summarized in the analysis of the survey.

researchers, standards bodies
Consultants
Managers of the service being "PKI Enabled"
IT security
Business Managers and the auditing community

Appendix F. Comments on What the PKI TC or Others Could Do to Help Increase Understanding of PKI

The Follow-up Survey asked for comments on what the PKI TC or others could do to help increase understanding of PKI. The full text of these comments is included here. To preserve the privacy of the survey respondents, these comments should not be distributed beyond the PKI TC. However, they are summarized in the analysis of the survey.

Understanding is needed in two areas: 1) Being able to identify what applications are really a good match for PKI--too often PKI is used for things that don't really require PKI. Since the overhead involved in implementing PKI is non-trivial, this leaves a bad impression when a more simple method would as well. 2) Senior management in particular needs to understand that a properly implemented PKI is a valuable corporate resource--again this becomes a excercise in understanding what benefits PKI can provide and what applications are a good match for it.
NON-TECHNICAL EDUCATION ON WHAT PKI IS, WHAT IT COULD BE USED FOR, PROS CONS TO USING IN VARIOUS SITUATIONS, ETC.
Technologists should stop trying to explain how PKI works.
Different education path should be developed based on different user. For the senior mgmt, they would be looking at ROI as well as user demand. For the end user, they are looking at ease of use, and transparency. Thus, more seminars should be developed based on different user as well as market focus.
Senioor management has been frightened by the cost...solid cost justification and ROI would sway them.
I'm not convinced that starting by talking about public and private keys is helpful. Sorry that I don't have a good answer for where you should start.
Generally complex IT is poorly understood among senior management and IT management making them not able to make good decisions. For PKI it is even worse, in many cases IT management does not really understand what the decision about deploying PKI means. Education and
Communication & education campaign, especially about the value proposition to each of the parties (because it is different for each party)
Offer educational programs or seminar at low cost or even no-cost Make introductary materials readily accessible on the OASIS web-site
Business people understand well the benefits of a legally authenticated signature attached to a document (contract or whatever), which cannot be repudiated and where the integrity, of the received document, is guaranteed. The only message that business people need to be convinced of is that a PKI signature with supporting legislation will provide exactly that. I have found that any attempt to explain to business people how PKI technically achieves signature, non-repudiation and integrity kills this important and relevant message. I think the 'technical' message should be given a very low profile in explaining PKI.
A wake up call, senior management does not understand the complexity of such a system and the fact that only a limited number of people can support that system. They don't understand that continuous training is required for the support of those system.
Get the word out that PKI is not just cryptography. It proves I am who I say I am. It proves a document was signed by me. It is a mobile credential. It is identity management based on cryptography but it is a credential.
Most "end users" do not understand what PKI does. Especially most "end-users" do not understand the concept of digitally signing something, and the fact that such a signature can be as valid as a normal one. However, management often has no more understanding of eg. PKI than the normal user, and therefore making a (business) case for PKI will often fail solely because of management understanding. Proving a ROI to management is near impossible if

management doesn't understand the service that is being provided
see prior comments on SSL
No
Improve usability and portability. If certs are easier to use then they will come.
begin development of seminars/training to help transition business processes to PKI-enabled state. Just providing technical training or "overviews" isn't enough.
Dont let upper management sell PKI, they don't for the most part understand the technology.
Provide tutorials at conferences and online. Provide a step-by-step cookbook for setting up PKI with very low cost for testing.
Show benefits and ways that applications could use a simple PKI technology to implement, protect and secure their data/applications.
Poor understanding
As mentionned earlier. Focus on the end user and what he/she may do in the PK-enabled systems and the savings and added functionality for senior levels.
Investigate and publish on the benefits on PKI, related to costs. Compare PKI to alternatives, such as username/password, one-time-password tokens etcetera. Maybe an authentication growth model?
There need to be 2 educational streams - one that is entirely business focused, and the other for technical specialists. As with other technologies, people need to understand that policy and process clarity must precede technical implementations.
PKI investment is hard to adjust its ROI. People even start to view PKI as "legacy application".
Good, honest, unbiased white papers. The 'trade press' published lots of articles that says "it's too hard"; where are the rebuttals? Where is the management level white paper that says "This is what asymmetric cryptography can do for you and this is how you take advantage of that" ?? (I don't mean sales hype that overstates the benefits and often misses the point altogether.....)
emphasize applications where encryption or validation of sender is required.
continue producing 1 pager education documents to descibe pki, from various viewpoints, eg user, implementor, management, support
Decision makers understand ROI, explain how the technology will deliver savings etc. and they will soon sort out the technology
Develop a way to discuss PKI in a non-technical manner. Such as a good flow diagram that a senior manager could review and have a business understanding of PKI.
Provide a primer on the subject defining PKI, and describing the issues.
Help make it easier to use and more "black box". Most people don't understand how a car works, yet they are proficient users of cars. PKI needs to evolve to be turn-key for all but the developers and IT architects and implementors.
While most people don't need to know exactly how it works, more Could be done to educate potential users of the unique benefits that only PKI can provide. In addition to digital signing and encryption (that Require the use of keys), the combination of the strong technology, strong policy and content rich credential (certificate) have distinct advantages over other security mechanisms that allow it to be very interoperable, both within different security domains within an enterprise (SSO, VPN, etc.) but also outside the enterprise as well. The "killer-app" for PKI is not one single application, but rather its ability to be used for many different applications within different domains. In short, the killer-app for PKI is utility. Unfortunately, more applications are needed out there to realize this.

Appendix G. Descriptions of Other Places Where Interoperability Problems Arise

The Follow-up Survey allowed respondents to enter descriptions of other areas where interoperability problems arise during PKI deployment and usage. The full text of these descriptions is included here. To preserve the privacy of the survey respondents, these comments should not be distributed beyond the PKI TC. However, they are summarized in the analysis of the survey.

Signature Cross-Validation
Legal issue
proprietory cert extension or OID
Differences in implementation of the same standards by various vendors
Between user applications
Certificate recovery
Certificate profiles. Such as unique, but meaningless (!) subject names. No usage of e-mailadresses for instance.
signed data objects
Policy Interoperability (not necessarily the same as cross-certification)

Appendix H. Comments on Interoperability Problems that Respondents Wanted to Highlight

The Follow-up Survey asked for comments on interoperability problems the respondents wanted to highlight. The full text of these comments is included here. To preserve the privacy of the survey respondents, these comments should not be distributed beyond the PKI TC. However, they are summarized in the analysis of the survey.

Again, this comes down to consistent implementation of standards...
Signature Cross-Validation between different tools is poor because of (in our XML area) different interpretation of document canonicalization.
ONE UNIVERSAL PKI FORMAT IS NEEDED. MULTIPLE FORMATS ARE NOT USEFUL EXCEPT IN VERY NARROW SITUATIONS FOR A VERY SPECIFIC PURPOSE.
Different e-mail clients, different applications could not intercommunicate successfully.
Legal issue plays a significant role in interoperability. Whose CPS should we use? What is the reliability limit now? Between 2 countries, which law should come into effect if a problem is detected in one country? Personally, I dont think interoperability will be viable as there is too much legal as well as business issue. For example, why should I open up my territory for another CA?
You also miss interoperability between the PKI aand its supported applications...
Actually. I think that PKI is one of the areas where interoperability is quite a bit better than other areas.
proprietory cert extension or OID requested by applications of different brands. Differenet interpretation thus implemenation of cert profile among differnet vendors.
Take the example with document signing. If an organisation want to implement document signing they have to use a third-party plug-in. How big big is the opportunity that their business partner chooses the same third-party plug-in? Close to zero? With this approach, PKI will only be useful within a organisation.
How to set or handle the extensions of certificates. That's too much complicated. Critical or non-critical must not be used. All of the extensions put must be critical.
Certificate subjec vs. directory hierarchy. Many applications try to map the certificate to the directory entry in order to find more information about the certificate owner.
Please see my comments under PKI Support issues. I categorized Interoperability there.
See above comments
The labor intensive nature of the interop problem -- It's a very daunting task to continue to keep any interop effort up to date as the standards change, product versions change, etc.
Providing a person with a single signature containing multiple certificates and providing access to multiple services is key to the wide adoption of PKI. Cross-certification and standards issues are the significant barrier to this process. I feel that the removal of these barriers would promote a significant uptake in PKI use.
Certificate Management, post issuance. Key Archive
I find "the transparancy of interoperability" to be the greatest problem. Most all applications with PKI support, can be made to interoperate, and in a usefull manner, provided the user posseses the necessary IT skills and understanding of PKI. However, requirements regarding technical skills are so high, that existing "interoperability" cannot be usefully exploited by the general user.
Between vnedor products, i.e. Entrust vs. Microsoft
Signature and path validation in a multiple issuers exchange. CRL is not the solution, multiple methods, and multiple client interfaces.
The main interoperability problem is with (1) protocols between PKI client and CA Server(s) and (2) usage of PKI functions by applications, since currently each application handles local PKI functions and local certificate storage formats differently.
Specifications are often complicated and hard to implement, resulting in many bugs that affect

interoperability. Too many features and optional requirements and sometimes competing standards produced by the same working group!
There are too many certificate issuance protocols. This should be simplified, with everyone agreeing on only one to be recommended. Other areas noted above suffer from not enough standards (smart cards) or poor testing with existing standards (validation and revocation).
As certificates are held within a database, certificate recovery becomes an issue if the user doesn't have the necessary certificate information to locate the record associated to their certificate.
Political processes between competing CA systems in a country, essentially marked sharing is neccessary.
x.509 is too hard to keep up with
The usage of unique, but meaningless (!) subject names. No usage of e-mailadresses for instance. Controlling the Trust list in the users browser.
Revocation checking is not always available in PKI-enabled application. It's also difficult to check policy or CPS in the certificate extension.
Path Discovery
Also note that its not always the PKI pieces themselves that cause interop problems. OSes without central key stores that all apps use cause many of the headaches with all of the import/export needs.
I'd be here all day! Drop me an email for interop problems
Interoperability with legacy systems. PKI tends to require a big bang roll-out and this is insane.
In eBusiness sharing certificates and signed documents beyond the enterprise.
Vendor differences. With the state we deal with several outside entities that may be using different PKI. We can not tell all entities that if they want to do electronic signatures with the state that they must use this PKI and we can not, finaicially, support and accept all types of PKI.
For PKI, interoperability is almost strictly a function of policy. X.509 has been around for a long time, is understood and accepted. What has been missing is a similarly consistent view toward policy. Ultimately, accepting a certificate comes down to a trust decision based on how much due diligence went into confirming the identity of an individual (as described in their certificate policy), and what recourse a relying party may have in the event the policy was not followed and there is a loss. In order for there to be interoperability, each CP must outline some measure of enforceable accountability on the part of the issuer in order to drive up the level of trust associated with a given certificate.

Appendix I. Comments on What the PKI TC or Others Could Do to Help Improve Interoperability

The Follow-up Survey asked for comments on what the PKI TC or others could do to help improve interoperability. The full text of these comments is included here. To preserve the privacy of the survey respondents, these comments should not be distributed beyond the PKI TC. However, they are summarized in the analysis of the survey.

Agreed upon implementation guidelines and possibly some sort of interoperability testing group (the SET vendors themselves formed an I14Y interoperability testng group and tested among themselves to work out interoperabioity problems. I believe that there are other testbeds as well....the 'opportunity' would be to get the vendors to agree that this would be a valuable project. From a consumer point of view, I would be highly desirable to know when doing product selection that certain products could demonstrate interoperability.
WORK TOWARD NATIONAL PKI STANDARDS.
I feel that more work should be done on the Legal issue to resolve this interoperability problem. It should cover business law as well.
See my "standards" statement, above
base guideline / blueprint from functional level on top of the tehnical standard ,eg. blueprint for a x509 cert to interoperable for web service authentication etc.
RFC3280 is too complicated. And I think that it only defines the profiles of certs or CRL, so we need more documents on how to use PKI, certs, and so on.
See above comments
Produce profiles for industry relevant standards and make recommendations when there are competiting standards. This will help to reduce the number of variables that can change interop results. Sponsor interop festivals or on-line reference implementation test sites which make it easier for vendors to do interop.
I know that standards and interoperability issues are high on the OASIS agenda.
Key Archive standards development covering key archive and recovery.
See 4.c above
See above comments.
Develop a way to locate the certificate holder's information, with strong authentication, so the certificate can be recovered and reused.
Enable global VA :-)
stop creating new extensions to certificates in x.509 - vendors cannot keep up. ASN.1 is hard - move to XML
Define guidelines for the topics above.
Smart-chip standards! NIST started with an API but there needs to be a connector-level auto-identification standard so that every platform O/S can interact with ANY smartchip just like it can now with any disk drive or digital camera.
Provide a specification which, for example, a secure email client requires to support in PKI to work. Once this standard is in place, PKI will be used
see previous responses.
Again, look at what the Federal government and other successful adopters of PKI have done and embrace those practices. From a technical standpoint, insist on portal products that have the ability to process certificate validation from a number of extra-enterprise CA's.

Appendix J. Other Comments or Suggestions

The Follow-up Survey asked for other comments or suggestions, especially ideas for how to address the obstacles listed in the survey. The full text of these comments is included here. To preserve the privacy of the survey respondents, these comments should not be distributed beyond the PKI TC. However, they are summarized in the analysis of the survey.

X.509-style digital identity certificates are the wrong solution for many applications. The PKI industry does not make it easy for prospective buyers of crypto-security products to make a choice that suits the particular requirements of their application; on the one hand, they realize that a crypto-less approach is insufficiently secure, but on the other the identity certificate approach is very heavy-weight. Often, one does not need all the elements of a PKI in order to solve ones application security problems; notably, light-weight attribute certificate solutions are more effective for many applications, yet the industry does nothing to promote the research and standardization of these. Dr. Stefan Brands
I think PKI efforts based on X.509 are completely mis-placed. The notion of non-repudiation is bogus. Digital signatures as document signatures are inappropriate. PK technology is very important, but not the way X.509 envisions it.
I would just reiterate the necessity of strengthening the standards to which the PKIvendors adhere (probably through some certification mechanism) and making the process, especially for users, transparent...to send a secure e-mail, all I meed to do is hit a button on my client and that is it...
In the RCMP, we have been our PKI in an operational environment since April 1996. We found that we were needs driven. That is our members required a means of secure communication in many different police operational areas. We had a solution for them, PKI. We addressed the urgent needs first with classroom type training. At the same time we sent out information about PKI and what operational problems it can solve. More needs came forward and were solved using PKI technology. In our organization we found that if we showed our members how to make their jobs easier to do, make them more productive and SECURE at the same time, most obsticles were easily taken care of. We found that training our members was the greatest challange since we are scattered from coast to coast. So we held train the trainers sessions in each province where at least 10 members were trained. Then they in turn would train the memebrs in their province. Although we have CBT's, we found that not many would take the time to take the CBT course. They prefered a classroom type setting where they could ask questions. Our training consisted of a full day. The morning to explain what PKI is, how it's used and how it makes members more productive solving operationa problems in a secure manner. This was very well received. The afternoon was focused on how to use Entrust and the various functionalities. We found that when your solution oriented, you can over come most if not all obstacles. We now have over 17,000 users on various applications other than e-mail. Training our Central Help Desk was another area we found to be very useful. If anyone in Canada has any problems with Entrust or using Entrust, they have one number to call and the CHD people can help with most problems. Those complicated problems are passed on to our level 2 PKI support and last to level 3. This works very well for us. We have integrated our PKI technology with a number of inhouse applications and have set up VPN's using Contivity. Once our members understand the technology, know how it can help them, they are on board and grateful for the help. Just some thoughts off the top of my head.
The benefits of PKI over SSL needs to better understood by business decision makers from a risk/business point of view. Techies get it. It is however quite expensive when one considers the entire cost equation (hardware, software, facilities, contractual framework, liability, high availability operations, staff, governance etc). Thus the only way to get more usage is to promote the benefits on the business side and the more cost effective approach of an outsourced model, supported by reference cases.
The previous survey was very high level and did not provide much new information. Would like

to see more details relative to PKI.
PKI TC should do three things: A. Create standard set of specifications for four aspects: (1) Functionality of the PKI client, (2) PKI APIs/methods to use PKI services by applications, (3) Functionality of CA Servers (Local CA Server, Policy CA Server, Top CA Server), and (4) Protocols between PKI client and different CA servers B. Promote A. with PKI vendors and application developers so that different PKI products are interoperable out-of-the-box and all applications are immediately PKI enabled, also out-of-the-box C. Promote usage of PKI and PKI-enabled applications within (first) its member companies with their products and also (second) with all their customers
It is clear at this point that PKI will survive and be invaluable as a security and prolific authN solution. The need to have better portability is driving the smart card / software vendors to support these devices. There really needs to be more buyin of standards based by Microsoft.
Thanks, Steve!!
Realise that a lot of PKI implementors and architects are contractors who cannot get open access to the Oasis work. This is the problem which the PKI Forum failed on.
In my view there are two problems with PKI: 1. The legal bar has been raised so high that implementation is difficult and costly. Compare this to the security and cost of a "wet" signature that digital signatures are supposed to replace. 2. PKI within the enterprise is tricky but doable. PKI beyond the enterprise (where the value of the extended trust the PKI offers is greatest) is very hard to implement because of trust issues between disparate CAs and lack of standards (and interoperable clients) for digitally signed objects beyond email.
I beleive PKI is a vaulauble tool that will assist in making all more efficient. We just need to make it costt effective and ensure interoperability for the end users.
Improving PKI is all about sweating the details. The technology is fundamentally sound, but currently implementing it is like "death by a thousand pinpricks". The lack of proper support in end-user operating systems and applications are the primary offenders.