Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Public Key Infrastructure Issues in an Academic Healthcare Setting

Planning a Public Key Infrastructure (PKI) deployment in a healthcare environment is a challenge that has unique aspects, determined by the nature of the healthcare business and by the user community the PKI intends to support. Addressing a mixed environment, academic and healthcare, adds complexity to the problem because of the mixed IT infrastructure likely to be seen in such environments and because of user education issues. The paper intends to give a general overview several specific issues related to the PKI depl...

Copyright SANS Institute
Author Retains Full Rights

AD

Public Key Infrastructure Issues in an Academic Healthcare Setting

Liviu Groza
Ver 1 September 2001

Summary: Planning a Public Key Infrastructure (PKI) deployment in a healthcare environment is a challenge that has unique aspects, determined by the nature of the healthcare business and by the user community the PKI intends to support. Addressing a mixed environment, academic and healthcare, adds complexity to the problem because of the mixed IT infrastructure likely to be seen in such environments and because of user education issues. The paper intends to give a general overview several specific issues related to the PKI deployment process emphasizing the particularities of a mixed environment. We assume that the reader is familiar with the functions various components of a PKI should perform.

1. Intro.

The healthcare industry has an obvious need for maintaining the confidentiality and the integrity of the information it handles, and such need together with an effort to standardize practices are being transferred into a legal framework by recent regulations (specifically HIPAA [1]). However, compliance with the law can be achieved in more than one way and when it comes to implementing changes that will lead to law compliance economic factors usually take precedence over the standardization effort. As a result of this situation, everybody agrees that PKI is a central component in a security conscientious organization but there is no implementation schema that will work for everybody and no unanimous agreement on what a PKI should provide.

In "PKI in Healthcare"[2] partners from 5 states were interviewed on 28 questions related to their PKI efforts and consensus was reached only over 16 of the 28 statements. In an academic healthcare environment it is very likely that some of the users in their dual role as academics and healthcare providers are being served by two separate IT departments with different views and missions, one serving the academic community and the other supporting the healthcare community. This being said it is even less likely to achieve a common vision on PKI requirements and implementation. There are two ways to get started in such a situation. One is to plan on educating users to distinguish between their 2 roles and use certificates and credentials accordingly (which can lead to situations where is unclear which role should be assumed). The other way is to have the user assume just the role that is more restrictive, (which can be a serious impediment in daily, more liberal business activities). Our opinion is that a decision on this question should be reached at the very beginning of the PKI planning process since it has implications on the whole architecture of the PKI.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

2. Planning

Once the need of a PKI defined and accepted at higher management levels into an organization a member of the IT group will be designated to lead the project that will make PKI reality into the organization. For simplicity we'll call the project leader ***"you"*** and if you are reading this there are chances that ***"you"*** is in fact simply you. What follows is mostly a list of recommendations based on the realities of an academic institution that provides healthcare services

Evaluate applications that will use the PKI:

You probably have a mixed situation when it comes to the applications supporting the business process. How many times have you been listening to PKI sales persons that say their product does a great job providing the infrastructure for certificates but you'll have to worry about integrating and using the certificates into the applications? And while your applications are not necessarily old (or not all of them), when it comes to rolling out new features the process is much slower that with other software products, and some time for good reasons. You can deliver (or buy for that matter) the most solid and reliable PKI, but you must first evaluate the applications that should take advantage of it and build your PKI accordingly. For the applications that are not ready to use certificates it is a good idea to at least get in touch with the vendors and get a feeling about when and how they are planning to implement them. In some cases the users will access applications or services provided by the academic IT department (email, maybe web services, etc). Whether or not and to what extend the PKI you are building will support these applications is a question to be answered at this time and not because of technological limitations but because of user education that may lead to higher levels of breaches in confidentiality.

Build a team. Interfacing.

You should get to choose the people you will be working with. This will not be a short project and it will have a lot of custom and nonstandard features so try to get staff that you can keep for a while. There were PKI pilots shutdown or even completely redesigned because of staff turnover (see [3]). PKI interoperability, which will mark the maturity of the implementations, is expected to be achieved in 2-3 years (see page 24 in [2]) and you better plan of keeping the core staff member for this period. Management support is also essential, as is involvement from the parts of the organization that deals with application support and user support. If you plan your PKI in conjunction with the academic site of the enterprise and if the IT departments are two separate entities, for this project there should be very good communication at technical level, as well as managerial since the final PKI should obey and implement policies coming from two sources.

Five perspectives of PKI.

These are the five main things that you should take into account and consider satisfying for a successful and acceptable PKI implementation (see Chapter 2 in [2]).

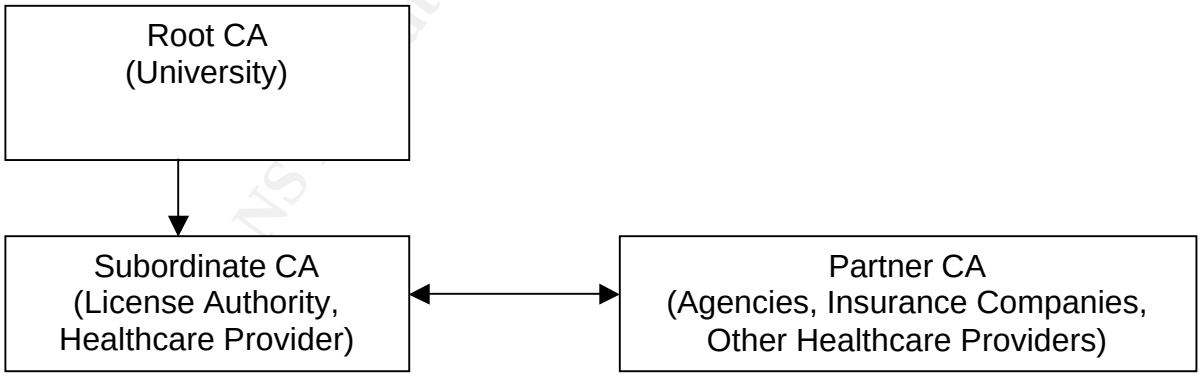
- Privacy policy. The PKI should implement the policies in place at your organization. Both the policies governing the activities of the academic side and of the healthcare side should be reviewed and renewed if necessary. Care should be taken

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

not to have conflicting regulations. It is a good idea to write a document referring to the objectives the PKI is trying to achieve, the policies it will implement (see below) and the laws it will be compliant with. Have a look at PKILaw.com [4] for an overview of laws governing the PKI. Having high management approval on such a document will give your team direction and it will also shield it from pressure likely to be seen later in the implementation process. This is even more important when dealing with two different management structures.

- User perspective. An important aspect for a successful implementation is the user acceptance. Keep in mind that this sort of products does not increase productivity, and they can be extremely easy misused. A good educational program is crucial but simplicity of the final system is also a must. Keep in mind the personality features likely to be seen your targeted user audience - healthcare providers are highly trained people, mostly non technical, extremely busy and with lots of responsibilities and things to worry about that every new thing that you try to get to their attention has to be really important or easy to use to be worth attention. On top of this, because of the academic environment, it is likely that your audience is accustomed or has been exposed to more liberal rules when it comes to the IT infrastructure and it is not likely to give away that comfort unless you can make a good case about it.

- PKI architecture. HIPAA is listed under "Administrative Simplification" on [1]. And one of the goals is to achieve data security by setting standards of interoperability. Since a single PKI serving the whole industry is not likely to be seen, the "bottom-up" approach where development starts at individual entities is the model the industry will follow. The technical implication to this is the use of a hybrid cross-certification architecture (see figure as well as [2], page 29). This will allow trust and accessibility to individual certificates from any entity in the network. Such architecture should in fact follow the legal responsibility and authority chain of the organizations involved. You should consider interfacing your PKI with the academic part of your business, which may already be part of a hierarchical certification structure as CREN [5].



- Inter Computer Communication. Due to the minimal effort required use certificates most platforms, email will be the first candidate to take advantage of the PKI. HTTPS will be another major player. Using server certificates it is possible to provide secure access to data (even on legacy systems) via web-servers and using client certificates stronger authentication can be enforced to webified applications that will require it. Most likely for these applications an in house development effort will be needed in order to get them to take advantage of the PKI in a timely manner.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Data representation. PKI will provide the backbone for secure communication but in order to achieve interoperability it is desirable to have the data in a non proprietary format (ASC X12, HL7 or XML are the recommendations in [2]).

3. Deployment Issues

We've seen that the desirable architecture for a CA is a cross-certified one. The CA of an academic-healthcare entity will usually be a subordinate of a root CA at University level which, for interoperability purposes, will have to cross-certify healthcare providers and partners that will cooperate with. This reality comes with several issues addressed in by Dave Barrnet in his paper [6].

Certificate Policy and Certification Practice Statement [7]. Two formal policies need to be adopted and one of their roles is to limit liability. The Certificate Policy defines the level of assurance to be placed in a certificate and its applicability. The Certification Practice Statement is a statement made by a Certifying Authority and outlines the steps it takes to verify the information it includes when issuing a certificate. All established Certifying Authorities have publicly accessible Practice Statements [8].

Inter-organizational agreements are requires by HIPAA when exchanging data between healthcare entities. Cross-certification is the technical implementation of the notion of mutual trust and the legal basis that will rely on is an Inter-organizational agreement.

Profiles.

When deploying a X509 v3 certificate we have the flexibility of using different options and extensions. These will constitute the certificate profiles and its flexibility prompts for matching profiles to real life user roles. This approach while mimicking the structure of a given organization can generate interoperability problems. The number of profiles should be kept to a minimum and a standard should be proposed it should be embraced.

Another major implication of user roles is the need for multiple certificates. At least two functions a user can perform require two different certificates to implement: encryption and digital signature. While keys used for encryption will most likely have to be escrowed, for non-repudiation purposes keys used for signing should not be escrowed. You may also find suitable to differentiate between keys used for encrypting communication and keys used for storage encryption.

Access to certain applications or levels into an application can be based on more sensitive roles that will require different "grade" certificates with different key usage and increased controls (bio-authentication) to use the key. As shown, profile and certificate proliferation poses a problem for administrators and for users as well. The users will have to figure out which certificate to use and the administrators will have more certificates to manage plus will have interoperability issues.

Users in a healthcare-academic setting will most likely be entitled to have certificates issued from two different sources thus adding another degree of complexity to this existing problem.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Privilege Management

Certificates bind an identity to a public key, identifying the owner. In order to perform different functions the (now identified) owner of the certificate needs to have a certain privilege level. We saw that we can embed privileges into standard X509 certificates by the means of "key usage".

Another way to manage privileges is to through decoupling the authorization and the authentication information. The industry is looking at implementing this idea through Attribute Certificates or Authorization API, which will describe and help manage the privileges separately.

A separate component that will globally manage the authorization for different applications throughout an enterprise is called Privilege Management Infrastructure. Having a separate service, dedicated exclusively to Privilege Management is desirable for many reasons. But PMI is bound to have almost the same integration problems as PKI, and when it comes to mixed environments the technology should allow for privilege checking on different infrastructures. A teacher who is a doctor should be able to access the academic PMI to get authorization to check student work and the HealthCare's PMI to access patient records. The practical problem at least for now is the immaturity of the standard and the fact that for the current time frame very few major applications are supporting it. Nevertheless this component should be followed and PKI deployment plans should leave open the opportunity to integrate with future PMI, when reaches maturity.

The Right Time.

Time stamping services should be part of a complete PKI for a variety of reasons. The immediate reason is the need to check revocation lists and certificate validity periods. Using timestamps within applications can have significant legal implications (the time a pharmacy order has been issued and signed, the time a procedure has been approved, etc). As with the paper process where date and time is sometimes part of the signature, digital signatures can make more use of the time service than the encryption process. The non-repudiation function a PKI should support has a time component as well. Use certified third party time stamp services or build and certify your own but the important thing is to have a way to prove that the time service itself is reliable and accurate within a given tolerance.

The Time Factor in Encryption.

Two issues are related to long time storage of keys. One is the storage of the key itself, and the other is the key vulnerability. Record retention is regulated by policies and mandated by law. In certain cases we are looking at time periods in the order of decades up to a century.

Obviously, to make use of an encrypted medical record one should have the means to decrypt it.

It is common knowledge that braking an encrypted message by brute force is just a matter of computational power. What we call secure is in fact "secure now, given the resources commonly found". The situation changes and it is advisable to review the key strength and eventually re-encrypt records with a key of a more appropriate quality. Making a business case for such a need is helped by the fact that media itself

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

deteriorates and as periodic transition to new media will be required, this can be accompanied by re-encrypting archived files.

Special care has to be taken to maintain decryption capabilities. As software changes the situation where you have the encrypted content but the software used for decryption is no longer available can be foreseen, especially for nonstandard encryption schemes.

4. Conclusions.

Technology for building the components of a PKI is becoming more mature. The main issues related to PKI deployment in healthcare and academia are mainly architectural and have a strong legal component. A good definition and understanding of the rules governing data (patient records) and data ownership and access is crucial in defining the needs and the future architecture of the PKI.

---

[1] PUBLIC LAW 104-191 AUG. 21, 1996 see also http://aspe.os.dhhs.gov/admnsimp/

[2] The HealthKey Program - PKI in Healthcare Drummond Group, http://www.healthkey.org/library/PKI-May-15-2000/PKI-May-15-2000.doc

[3] National HealthKey Project - Pilot Projects Information http://www.healthkey.org/what-works/index.html

[4] PKI and the Law http://www.pkilaw.com/

[5] Corporation for Research and Educational Networking http://www.cren.net/ca/index.html

[6] Public Key Infrastructure Concerns in Healthcare Settings - Dave Barnett, Kaiser Permanente http://www.tunitas.com/pages/PKI/docs/PKIConcernsinHealthcare.pdf

[7] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, ftp://ftp.isi.edu/in-notes/rfc2527.txt

[8] Thawte's Certification Practice Statement at http://www.thawte.com/corporate/cps/cps.html; Verisign's CPS at http://www.verisign.com/repository/CPS/

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced