

The Use of PKCS-12 in the Federal Government

Tice F. DeYoung, PhD

National Aeronautics and Space Administration

INTRODUCTION

The purpose of this paper is to provide a brief description of the history of the Public-Key Cryptography Standard number 12, or PKCS-12, the Personal Information Exchange Syntax, for exporting public key infrastructure (PKI) private keys and certificates; to investigate the implications of using this mechanism as they apply to the Federal PKI Policy Authority; and to present a set of conclusions which are not recommendations *per se*, but are rather a list of things to consider before one permits end users to export their PKI private keys and certificates using PKCS-12.

BACKGROUND

Before we describe PKCS 12, we should first mention what the Public-Key Cryptography Standards are. These specifications are produced by RSA Laboratories in cooperation with a number of developers worldwide for the purpose of accelerating the deployment of public-key cryptography. The first PKCS was published in 1991. Since then the PKCS documents have become widely referenced and implemented.

THE PKCS-12 STANDARD

To understand how PKCS-12 came about, we have to go back to 1995. At that time all of the encryption software was proprietary and there was no mechanism for people to securely communicate unless they had the same product. This lack of interoperability was recognized by a number of people.

There were several development options that could lead to interoperability. First, you could set up a new application specific certificate authority (CA) to issue PKI certificates for every user of that application. Second, you could develop application specific plug-ins for every other application. Because each of these options leads to unnecessary complexity and/or expense, the community arrived at the best option; they all agreed that a single standard should be developed. That standard came to be known as PKCS 12, published by RSA Laboratories in 1999. [1]

The PKCS 12 standard built upon and extended the 1993 PKCS 8: Private-Key Information Syntax Standard [2] by including additional identity information along with private keys and by instituting higher security through public-key privacy and integrity modes. The PKCS 8 standard described syntax for private-key information, including a private key for some public-key algorithm and a set of attributes, as well as, syntax for encrypted private keys.

The PKCS-12 standard describes a transfer syntax for personal identity information, including private keys, certificates, miscellaneous secrets, and extensions. Applications that support this standard will allow a user to import, export, and exercise a single set of personal identity information. This standard supports direct transfer of personal information under several privacy and integrity modes, the most secure of which require the source and destination platforms to have trusted public/private key pairs usable for digital signatures and encryption, respectively. PKCS 12 permits both software and hardware implementations. Hardware implementations offer physical security in tamper-resistant tokens such as smart cards. [1]

FEDERAL PKI POLICY AUTHORITY

The Federal PKI Policy Authority (FPKI-PA), under the auspices of the Federal Identity and Credentialing Committee (FICC), is responsible for the policies of the various Federal PKI implementations; the Federal PKI Bridge CA (FBCA), the Common Policy Framework CA (CPFCA), the eGovernance CA (eGOVCA) and the Citizen and Commercial Class CA (C4A). This paper will only discuss the relevancy of the FBCA and its concomitant Certificate Policy to the use of PKCS 12.

The Federal Government is required to use cryptographic modules that have been accredited as meeting the NIST Federal Information Processing Standard 140 level 2 (FIPS 140-2) accrediting process [3]. Additionally any entities PKI that want to cross-certify with the FBCA must follow US Government PKI Cross-Certification Methodology and Criteria. [4]. Once an entity PKI has completed this process, they are required to sign a Memorandum of Agreement (MOA) with the FPKI-PA, which lays out the rights and responsibilities of both parties. One of the items in every MOA is the requirement that the entity PKI cross-certifying with the FBCA shall maintain compliance with the requirements in the MOA and shall notify the FPKI-PA if any material changes occur.

ISSUES WITH THE USE OF PKCS-12

The FBCA Certificate Policy [5] is silent on the use of PKCS 12, so that its use does not apparently violate any of the requirements in the MOA. However, as we will discuss later, there are issues associated with private key protection and activation, which are application specific that must be addressed. One of the questions that arises is whether or not an entity must notify the FPKI-PA if it intends to use PKCS 12; another is whether the entity must notify the FPKI-PA of every application that it intends to import the PKI secret keys and certificates into. There are others, which will be discussed in more detail in the following sections.

Exporting the private keys and certificates isn't the problem. PKI applications that follow the PKCS-12 standard keep the exported data in an encrypted state. To further explain this, let me use an analogy. Let's assume that the PKI application is equivalent to a safe, because the private keys and certificates are maintained securely, in one place and easy to centrally manage. When the information is exported, it is no longer in the safe, but is in a portable lock box, or secure briefcase, which is portable. The container is protected, so that doesn't cause a problem. However, the portable container can be used in an insecure fashion if it isn't carefully controlled.

Let me use as an example the FBCA CP Medium Level of Assurance requirements. The FBCA CP requires private keys to be protected with FIPS 140-2 accredited devices and applications for cross-certification at the Medium Level of Assurance. I use this example because the overwhelming majority of entities cross-certified with the FBCA and those who have applied for cross-certification have been at this level. Furthermore, the Medium Level of Assurance at the FBCA covers both Levels 3 (software PKI) and 4 (hardware PKI) as outlined in the OMB Guidance on Authentication Levels[6] and the associated NIST Electronic Authentication Guideline[7]. For this example I am assuming that the PKCS 12 exported PKI data is secured in accordance with FIPS 140-2. Therefore, exporting the PKI data from the PKI application (safe) to the PKCS-12 container (secure briefcase) has not violated the FBCA CP requirements. One of the FBCA CP requirements is that passwords used to unlock access to the private PKI keys must be at least 8 characters in length and contain at least one from each of the following categories (upper case, lower case, numbers and special characters). This requirement is easily met when the private key data is

in the PKI application and when the data is exported using PKCS-12.

Now things begin to get interesting. While within the PKI application, the keys and certificates are centrally controlled and managed. However, when the PKI data is exported, the PKI applications are now unable to provide this management because they have no control of the portable PKCS-12 container, nor do they control what applications and devices the private keys and certificates are imported into. The end user is the only one who can control things once they have been exported. Therein lies the rub! The end users will have to maintain consistency between their keys and certificates that have been exported and those that are still within the PKI application. They will have to keep track of updates, key rollover, what applications and devices they have exported them to, etc. They are also the only ones responsible for determining if the applications and devices meet the FIPS 140-2 requirements. How can we ensure that the end users maintain their exported PKI data in a manner consistent with their CP and CPS and their FBCA MOA?

This brings us to the next section of this paper, namely the things one should consider before allowing end users to use the PKCS-12.

THINGS TO CONSIDER

First and foremost, you do not want to do anything that will cause your use of PKCS-12 to violate the level of assurance of your CA and, if you are cross-certified with the FBCA, you don't want to jeopardize the MOA requirements you have with the FPKI-PA; so tread carefully if you do decide to permit PKCS-12 export of private keys and certificates.

What are the benefits of permitting the use of PKCS-12 mechanism for exporting private keys and certificates? One that comes quickly to mind is that it permits you to import them into the Blackberry Personal Digital Assistant (PDA) beloved by upper level management in most Federal agencies. These devices are ubiquitous throughout the ranks of these Senior Executives who tend to be the least versed in information technology security issues. We have to provide them and their data without bothering them with details or interfering with their ability to properly lead their agencies.

Blackberries are only the tip of the iceberg when it comes to PDAs. There will soon be smart phones,

other intelligent PDAs and possible Personal Access Networks (PAN). The one thing they have in common is wireless connectivity. Wireless access points will rapidly follow and we will have to provide adequate security for these devices using some form of cryptographic mechanism. Having the same private keys and certificates for the myriad devices and applications is an efficient way to easily manage this. PKCS-12 gives you that capability.

Now, what can you do to ensure that giving your users this capability doesn't compromise your security and thus your level of assurance? First, review your CP and CPS to see if there are any changes required. Note that if you are operating at the High Level of Assurance, you cannot permit the use of PKCS-12 export or you will violate your policies. Second, notify the FPKI-PA of your intention and the steps you will take to ensure that you do not violate your level of assurance. Next, consider additional procedures and processes for the subscribers that will use PKCS-12 export. Here are a few suggestions, but this list is far from complete:

- A. Put the PKCS-12 users in a separate group;
- B. Use a separate OID in their X.509 certificates;
- C. More closely audit their usage;
- D. Require additional training in managing their private keys and in the procedures for exporting and importing them;
- E. Require subscribers to obtain permission from your agency Policy Authority (PA) before importing their private keys and certificates into an application or device;
- F. Develop a list of FIPS 140-2 approved applications and devices that would be the basis for your PA decisions in E.;
- G. Issue their credentials at the Basic Level of Assurance, but only if absolutely necessary to maintain cross-certification

- H. Develop a Supplemental Subscriber Agreement that describes their additional responsibilities and notifies them that extra training is required.

Here are some things you might want to include in the additional training for your users who want to use PKCS-12. Again, this list is for illustrative purposes only and should not be considered to be all-inclusive:

- A. Describe their responsibility for and methods of managing their exported keys and certificates;
- B. Explain that the users can only import their private keys and certificates into applications and devices that their PA has approved as meeting FIPS 140-2 requirements;
- C. Describe the processes and procedures to followed for exporting and importing their PKI data;

CONCLUSIONS

As we stated at the beginning, we are providing no conclusions or recommendations on the use of PKCS-12; but instead, have briefly discussed some things to consider before embarking into the brave new world of permitting users to export their PKI private keys and certificates using the PKCS-12 export mechanism.

However, for your information, we at NASA have carefully weighed the attractive benefits and the potential dangers of permitting users to export their private keys and certificates and have made the decision to permit certain users to use PKCS-12. We are now implementing some of the above steps to ensure that we do not compromise our security. We are cautiously optimistic that things will proceed smoothly.

REFERENCES

- [1] PKCS 12 v1.0: Personal Information Exchange Syntax, RSA Laboratories, June 24, 1999.
- [2] PKCS 8: Private-Key Information Syntax Standard, RSA Laboratories, November 1, 1993.
- [3] Security Requirements for Cryptographic Modules, NIST FIPS 140-2, December 3, 2002.
- [4] US Government PKI Cross-Certification Methodology and Criteria, March 2003.
- [5] X.509 Certificate Policy for the Federal Bridge Certification Authority, 27 September 2004.
- [6] E-Authentication Guidance for Federal Agencies, OMB 04-04, December 16, 2003.
- [7] Electronic Authentication Guideline, NIST Special Publication 800-63, v. 1.0, June 2004.