

# Throwing Rocks at the Public Key Infrastructure

## Simplifying the Forgery Process

**Eric Knight, CISSP**

**knight@securityparadigm.com**  
**Copyright © 2000 by Eric Knight, All Rights Reserved**

### **Introduction**

When I first heard about the idea of Public Key Infrastructure (PKI), I was both amazed at its potential and dismayed at the shortcuts being taken in its construction. While I believe that Public Key technology and the use of third party authentication is the correct solution, the ideas presented at conferences, in white papers, and in real-life applications are proof of hurried decision making. Instead of presenting only opinion, however, I'd like to illustrate the technical side of the issue and allow readers to draw their own conclusions about the safety of the current Public Key Infrastructure.

### **Understanding the Commercial PKI Problem**

Right now, PKI is one in a series of new technologies that is being implemented at web sites world wide, and no small amount of interest is being taken as to what people would like to do with it. Public Key has been given the go-ahead as an adequate replacement for teletype contracting in several states, as it supposedly provides enough proof of identity.

To demonstrate the nature of the certificates to the ability to contract with the keys, the following is taken from the USERTRUST Web Site, as a brief description of their personal certificate services:

The USERTRUST Network Secured Private Key Systems are digital signatures and digital signature products. The USERTRUST Network offers the following classes of e-mail certificates:

Bronze - Bronze certificates establish the users ID and can be used as legally binding signatures under Utah law and the law of 23 other states.

Silver - Silver certificates have all the benefits of Bronze, but establish the creditworthiness of the users.

Gold - Gold certificates have all the benefits of Bronze and Silver, but establish that the user has no serious criminal record.

Crown - The Crown certificate has all the benefits of a Bronze, but also establishes the users professional licenses or expertise.

Therefore, a person with such a key can contract for the owner without any additional representation even with just the "lowest grade" key that USERTRUST provides. The responsibility of protecting that key falls upon the key's owner. With 23 States (approximately half the United States) willing to accept this as valid, one would assume the PKI must be protected by bullet-proof security.

The greatest security issue of running a PKI company is dealing with authentication issues. After all, how do you really know the person on the other end is the person they claim they are? Because Privacy Act protected information is generally unavailable, actual proof of a person's identity is a costly if not impossible task. Substitutes to proof-positive validation are required in order to provide any security at all.

The commercial PKI approach will deviate much from a government supported PKI approach, considering that a government already has access to a rather extensive identity verification system. A government system would be able to support first-person meetings for key signatures, have photo identities, and access to Privacy Act information. Little need is required for substitutes to the validation system if the government is specifically checking.

However, the existing PKI is controlled by commercial entities, and as a result, the existing PKI does use a number of substitute methods in order to confirm identities. Therefore, it is reasonable to assume that the substitutes may be poor choices for the PKI security as a whole, and therefore the system may be vulnerable.

As an example, when you register for a common e-commerce grade key, you will see the following predominant security measures:

- The user's identity is validated by email.
- The user's keys are protected by a challenge phrase, or password.

As a professional computer security researcher, I have learned that email is extremely difficult to secure. SMTP servers have catalogued over 100 security vulnerabilities (see Figure 1), and all network engineers realize firewalling off SMTP stops the mail flow. A direct path to the SMTP system is therefore required, and is always a potential entrance into a firewall-protected network.

1022	<input checked="" type="checkbox"/>	Sendmail	<b>sendmail(8) 4.0</b>	Administrator Access
<p>A user's rhosts file can be overwritten using the following rcpt line:</p> <pre>rcpt to: /usr/users/joeuser/.rhosts</pre> <p>CERT(s): None</p>				
262	<input checked="" type="checkbox"/>	Sendmail	<b>sendmail(8) 4.1</b>	Administrator Access
<p>You could telnet to port 25 and enter the command "wiz", and if you responded to the server with the correct default password (assuming a non-frozen configuration file) then additional command were enabled as well as a shell. If the configuration file got from and there was no password information stored in it, then no password was required. Therefore, a remote user could get a root shell by telnetting to port 25.</p> <p>CERT(s): None</p>				
278	<input checked="" type="checkbox"/>	Sendmail	<b>sendmail(8) 4.1</b>	Administrator Access
<p>Exploit allows remote access as bin, and since bin owns the /etc dir you can gain root.</p> <p>CERT(s): None</p>				
1023	<input checked="" type="checkbox"/>	Sendmail	<b>sendmail(8) 4.1</b>	Administrator Access
<p>By making the sed program the recipient of email, the contents of the email message can be executed as a shell script.</p> <pre>rcpt to: &lt; sed 'l,/^\\$/d'   sh&gt; 250  sed `l,/^\\$/d'   sh.. Recipient ok data ...script CERT(s): None</pre>				

Figure 1: DMW Worldwide Inc. Vulnerability Database, clipping of some older Sendmail vulnerabilities

Furthermore, hacker attacks might not be the only source of potential site compromise – “disgruntled” internal administrators, network engineers, or consultants may also perform this trick because it is likely that they already have administrator access on the mail server.

Now that we’ve surmised that this system of validating the user of the Digital Certificate is not only exposed, but also historically “hackable”, and requires complete trust of the mail server’s administration, what exactly does this imply? We know that the source of identity confirmation could be compromised. Are key users now in jeopardy of having their key forged and their identities assumed by another individual? What tools does it require? And most importantly, which vendors currently employ a system that could be vulnerable?

## Exploiting the Public E-Commerce Umbrella

The first logical step after a mail server has been compromised would be to look for individuals with digital certificates. One would assume that certificates are kept under lock and key inside a vault somewhere; however, due to the lack of standards by various providers finding out who on a site has a key is trivial. The problem exists in the providers of certificate service, called a Source of Authority.

A Source of Authority (SOA) behaves as a third party in order to validate your identity to other people who are also validated by the SOA. Mathematically and theoretically, it appears that PKI and Digital Certificates are the “correct answer” and is considered solid security. What cryptography succeeded at establishing, however, didn’t take management practices and financial transactions into account.

What this design does not address is that managing a large number of users (1,000s up to millions of people) requires some “friendly” management features that may also yield more information than a small person-to-person SOA may have, making security compromises easier than fighting the mathematics.

Probably the most dangerous of which is revealing who is under the umbrella they support. It turns out that many SOA's will just give you that information, as demonstrated by Figure 2 and Figure 3.

### Search by Email Address or by Common Name

To find a certificate issued by us, just enter the user's e-mail address or his/her name and click on the Search button.

Enter the e-mail address

or

Enter the exact name:

Partial matching

---

Certificates:  operative  revoked  
 expired  pending


Figure 2 – GlobalSign's Search Engine for Keys



## Digital ID Services

### Help with this Page

The query returned the following matching certificates. Clicking on the name link will allow you to view more detailed information about the certificate or perform additional operations on the certificate such as download, revoke, renew, replace or set preferences.

 This icon next to a listing indicates that the Digital ID is the owner's preferred certificate for encrypting secure messages.

**Tom Danner** (Expired)  
tdanner@dmwgroup.com  
Digital ID Class 1 - Client Authentication Standard  
Validity period from Aug-25-1997(GMT) to Feb-24-1998(GMT)

[New Search](#)

**Figure 3 – An example of the results of a search from VeriSign’s Certificate Repository**

Even if this method does not allow wildcards to be used, it does allow the intruder to compile a list of available site key holders from the compromised mail host, without ever examining the user’s computer for signs of a key. I believe having this information public is far too convenient for attackers.

## Forging a Duplicate Key

Now that we have a list of all the users with Digital Certificates, what options do we have? If a key is lost, destroyed, or stolen then the key should probably be completely reassigned from scratch; however, this is not the case under the present SOA system. The only real proof of the original owner’s identity rests in the public/private key-pair originally generated, and if that gets lost, it is up to the SOA to reissue a new key.

It is often the case, however, that the SOA issues a duplicate key and treats it as if it was the original, instead of issuing a new key that requires critical identity reconfirmation. This is the largest opportunity for key forgery and, unfortunately, it does exist, as illustrated in Figure 4.



## Revoke and Replace Your Digital ID

This Digital ID is still valid. When you enter your challenge phrase and click Continue your Digital ID will be revoked and you will be taken to a replacement enrollment form. It is not possible to revive an Digital ID once it has been revoked. If you are trying to replace a Server ID, please make sure that you understand the qualifications for replacement before proceeding. If you do not wish to revoke and replace this Digital ID, use your browser's back button to return to the previous page.

By submitting this request, you accept the terms of the [Relying Party Agreement](#).

A screenshot of a web form with a yellow background. It contains the text "Enter your challenge phrase and click Continue." followed by a text input field labeled "Challenge Phrase".

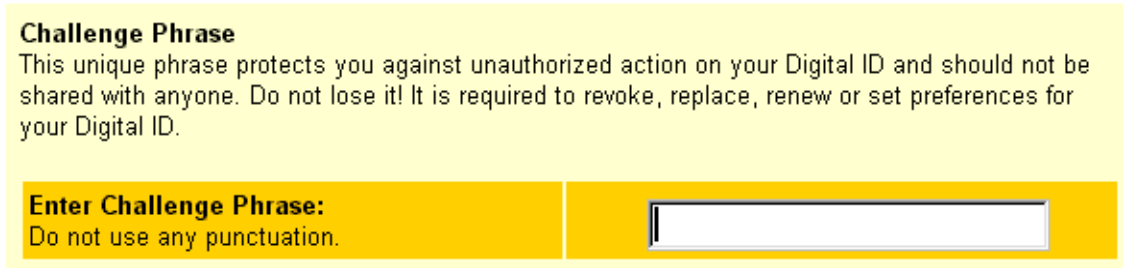
Click the CONTINUE button to revoke and replace your Digital ID.

Continue

**Figure 4 – Revoke and Replace Screen, showing a challenge phrase is only authentication needed**

## The Poor Password Problem

At this point, we have almost forged a key, but we still have several obstacles in our way. The biggest problem is the user password. Based on my experience in security and password cracking, breaking this password is not difficult, as illustrated in figure 5.



**Challenge Phrase**  
This unique phrase protects you against unauthorized action on your Digital ID and should not be shared with anyone. Do not lose it! It is required to revoke, replace, renew or set preferences for your Digital ID.

**Enter Challenge Phrase:**  
Do not use any punctuation.

Figure 5 – A typical password screen, this particular one displays “Do not use any punctuation”.

This challenge phrase clearly will be weak as evidenced by the directive not to use punctuation. If I enter a password only five digits long, in all lowercase letters, all the characters that I type for the password are displayed in cleartext on the screen, not only here, but on the certificate information form as well, automatically populated from this field. This is a very insecure mechanism.

It appears of the five SOAs that I present here, all of them had problems with passwords. Users could pick standard dictionary words, some were limited to how many letters maximum they could use, and none of them required at least a single special character or number.

## Intercepting Email

Once the form is complete, the next critical step is the reason why the mail system needed to be compromised in the first place. To complete the process, an email containing a challenge key will be sent to the key-holder’s address. This must be intercepted and, once intercepted, all the remaining steps used to duplicate the key will be automatic and unchallenged. The VeriSign email looks like this:

QUICK INSTALLATION INSTRUCTIONS  
-----

To assure that someone else cannot obtain a Digital ID that contains your name and email address, you must retrieve your Digital ID from Verisign’s secure web site using a unique Personal Identification Number (PIN).

Be sure to follow these steps using the same computer you used to begin the process.

Copy your Digital ID PIN number  
Your Digital ID PIN is: 44cef4ef9628863b019f43c516af8d60

Go to VeriSign’s secure Digital ID Center  
<https://digitalid.verisign.com/enrollment/nspickup.htm>


Paste (or enter) your Digital ID PIN  
Then select the SUBMIT button to install  
Your Digital ID.

That’s all there is to it!

It does not matter where your web client is for the generation of this key, even if the email came from Tokyo and then traveled to New York. The critical issue is that you confirmed the key's email identity and that was all that was required to create the forged key.

By going through the regular steps required by your browser, the new certificate is created. The new key is now the only working one, and the original key has been revoked. The result of this is demonstrated in Figure 7.

---




## Digital ID Services

---

Help with this Page

The query returned the following matching certificates. Clicking on the name link will allow you to view more detailed information about the certificate or perform additional operations on the certificate such as download, revoke, renew, replace or set preferences.

 This icon next to a listing indicates that the Digital ID is the owner's preferred certificate for encrypting secure messages.


---

**Eric Knight** (Valid)  
eknight@dmwgroup.com  
Digital ID Class 1 - Client Authentication Full Service Replacement  
Validity period from Dec-01-1998(GMT) to Dec-01-1999(GMT)

**Eric Knight** (Revoked)  
eknight@dmwgroup.com  
Digital ID Class 1 - Client Authentication Full Service  
Validity period from Dec-01-1998(GMT) to Dec-01-1999(GMT)

**[New Search](#)**

---

Copyright © 1998, VeriSign, Inc. All Rights Reserved 

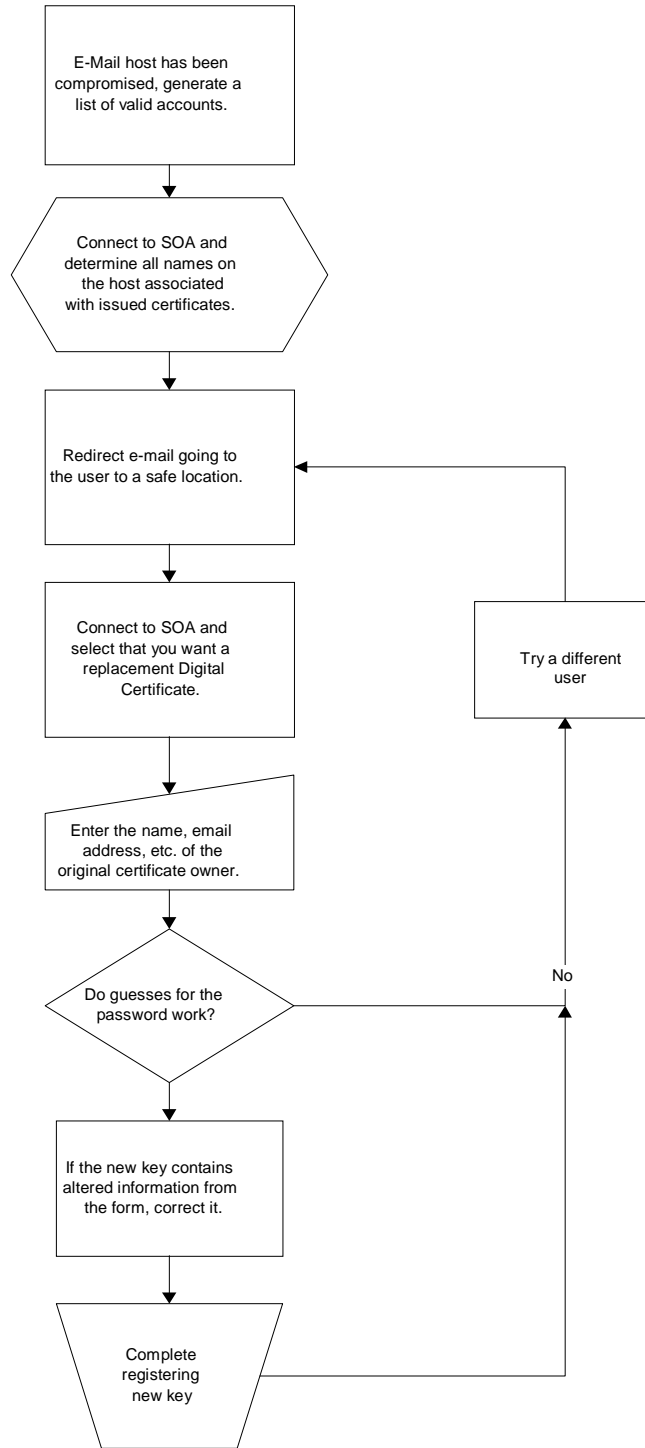
**Figure 7 – What a forged key looks like in the repository**

At this point, the attacker has assumed the identity of the victim and a forgery of the key now exists. In retrospect, the task would have been made considerably more difficult if the following were implemented:

- People were not allowed to arbitrarily check on the existence of certificates.
- People were required to pick a more secure password
- Email was not used as the sole proof and evidence of a person's identity

# The Flow

Here is a flow of the attack logic:



Attack Flow Diagram



## Other Interesting Observations

In the process of examining other implementations, I came across a few interesting tidbits of information. These are basically interesting derivations from the generally accepted practice of other SOAs.

**Thawte** asks a series of questions that the owner of the certificate must answer, so that the identity can be proven over the phone. However, this process is mainly for situations where an account has already been completely compromised. Also account ID names are generated from personal information, so that they are harder to guess.

If I were told to pick a “most secure” of the five services I examined, I’d have to pick Thawte. They don’t appear to have a public repository and assign a user id in a manner, although guessed with the right information, cannot be deduced from just the email server information alone.

Below are the questions and answers you have supplied to help you obtain a new password if necessary. If you see any mistakes simply use your browser "Back" button to correct them. This information is not permanent and can be changed in your "Preferences" page.

Question:	Answer:
How many pets do you have?	
What is your partner's nickname?	
What is your father's middle name?	
What is your mother's maiden name?	
What is your data line phone number?	

If you are satisfied that these accurately reflect your identity and preferences, press "Next". We will email you further instructions. As soon as you receive that email (you should have it immediately unless your mail is processed in batches) you should follow the instructions there to complete the process. Remember, you will need your password!

**VeriSign** and **USERTRUST** require a validated credit card purchase for a certificate, which isn’t actually a bad idea because it brings about a more complicated process with financial backing and verification. In many cases, trust equates to money, the more money the person spends, the less likely they are to abuse the resource. However, means of payment don’t necessarily equate to verification of identity, and in our particular attack model credit cards don’t even play a role, so even though this makes the system stronger it doesn’t solve the problem.

**GlobalSign** provided this gem, users are asked to supply a “hint” as to what their password is. I’m completely at a loss for words about a security company having something like this. This is a pretty good indication about the problems with PKI being too convenient as a whole.

Your password :	<input type="text"/>
Again for verification :	<input type="text"/>
Your password hint (*) :	<input type="text"/>

(\*) if you forget your password, GlobalSign will present you this password hint to help you remind your password. Example of a password hint : "the password is my place of birth"

## Conclusion

Although the Public Key Infrastructure currently contains some safeguards, its security has proven to be only as strong as its weakest links. The great security advantage of the Public Key Infrastructure is being held fast by convenience and insecure validation techniques.

## PKI Vulnerability Chart

	Public Listing of Users	User can pick any password	Email is Preferred ID Verification	Credit Card Required
Verisign	Yes	Yes, 5 char or greater	Yes	Yes
Thawte	No	Yes, 6 char or greater	Yes	No
TexStar Technologies	Yes	Yes (unknown lower limit)	Yes	No
GlobalSign	Yes	Yes	Yes	No
USERTRUST	No	Yes (no more than 8!)	Yes	Yes

## Resource List

VeriSign Corporation

[www.verisign.com](http://www.verisign.com)

Thawte

[www.thawte.com](http://www.thawte.com)

TexStar Technologies

[www.caserver.com](http://www.caserver.com)

GlobalSign

[www.globalsign.net](http://www.globalsign.net)

USERTRUST

[www.usertrust.com](http://www.usertrust.com)