

VeriSign Managed PKI Information Disclosure Vulnerability

Overview & Scope

This document will outline a vulnerability in VeriSign's web-based 'Managed PKI' system which allows unauthenticated access to some areas of an MPKI account where confidential information is exposed.

It can be used to gain access to the accounts of several high-level VeriSign partners, again, without any authentication. From within these accounts, key information is disclosed – the list of domain names registered to the account for that customer, and the contact information of the MPKI administrator. A complete list of all certificates issued by that customer can also be viewed and downloaded in a Microsoft Excel format.

A second vulnerability allows any unauthenticated user access to detailed information on any VeriSign-issued certificate, including the option to revoke the certificate. The revocation does require a 'challenge password' to complete the process, but this is unauthenticated and essentially reduces the security of any VeriSign –issued certificate to a publically-accessible password prompt.

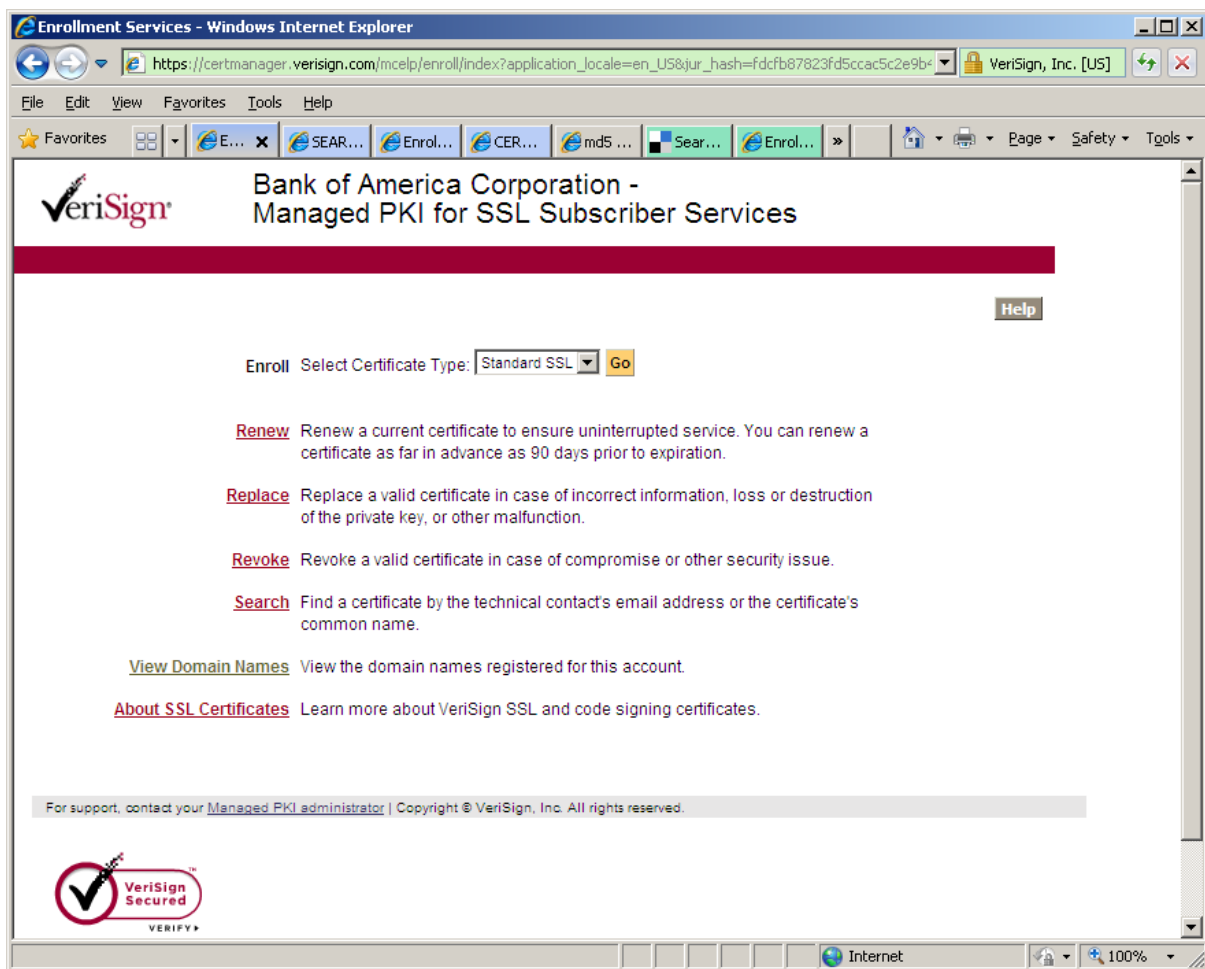
Vulnerability

i) Information Disclosure

VeriSign uses a 'jurisdiction hash' appended to the MPKI management URLs to allow login to accounts without providing authentication information. Thus, a simple URL such as:

https://certmanager.verisign.com/mcelp/enroll/index?application_locale=en_US&jur_hash=fdcfb87823fd5ccac5c2e9b4b80dd507

can be used to login to the MPKI account for Bank of America. (The hash appears to be a simple MD5 hash of the organisation name).



From within this account, there are at least two immediate information disclosure vulnerabilities.

- Clicking 'View Domain Names' shows a complete list of all domain names registered to the account – which could include some hostnames or domains that are not intended to be public information.
- The link at the base of each page ('For support, contact your Managed PKI administrator') contains an email address for the MPKI administrator – this is often not a publically-disclosed address.

ii) Certificate Revocation

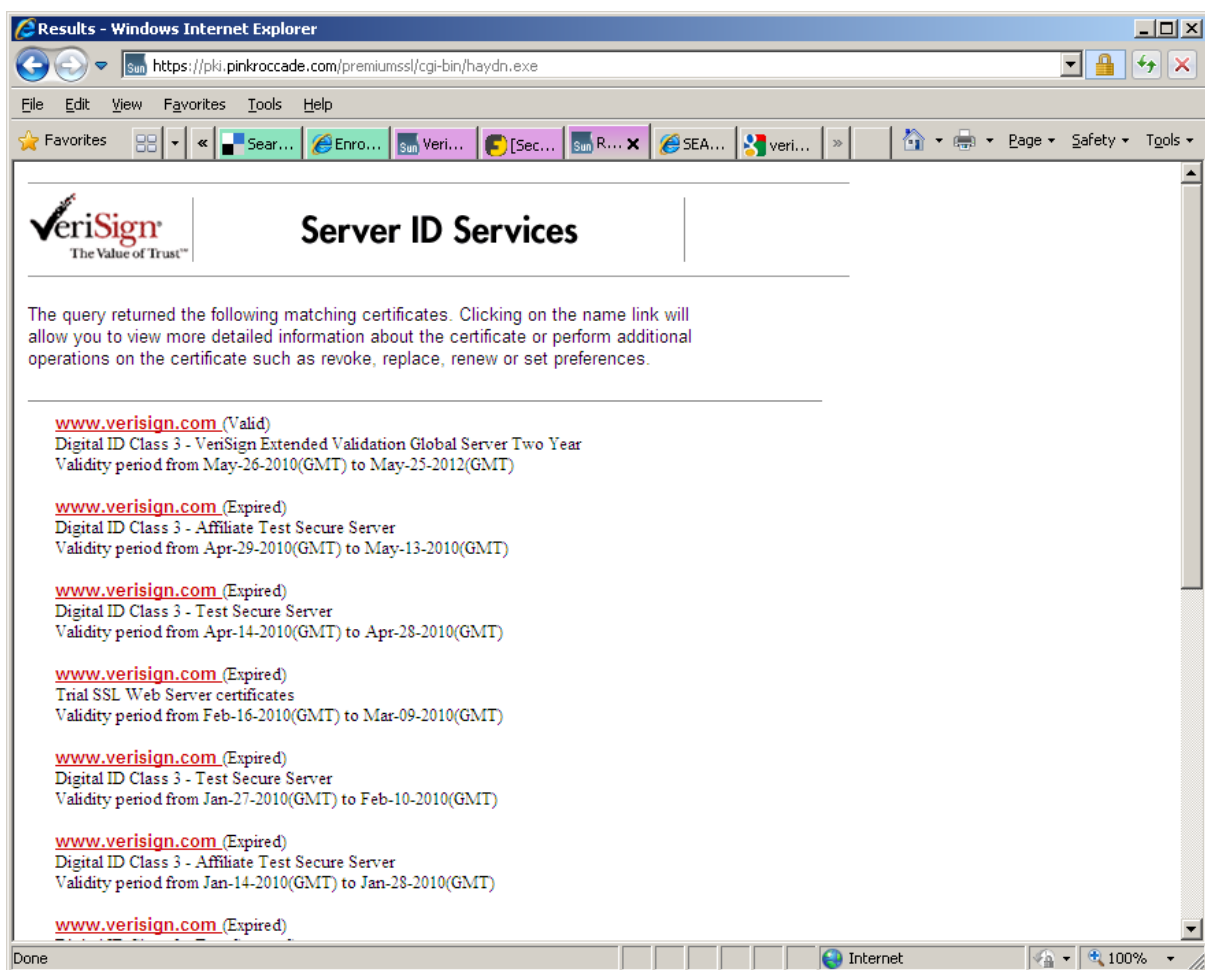
VeriSign offers a search facility to view information on any VeriSign-issued certificate. This search facility, enabled via a Dutch VeriSign partner (PinkRoccade) seemingly allows the searching and viewing of any certificate – not just those issued through PinkRoccade.

The search page is available here:

<https://pki.pinkroccade.com/premiumssl/services/globalserver/search.htm>

and is unauthenticated.

Searching, for example, for 'www.verisign.com':



You can see detailed (although public) information about the certificate. At the bottom of the page when clicking on an individual certificate, there are several buttons for certificate-management actions, including 'Revoke'.

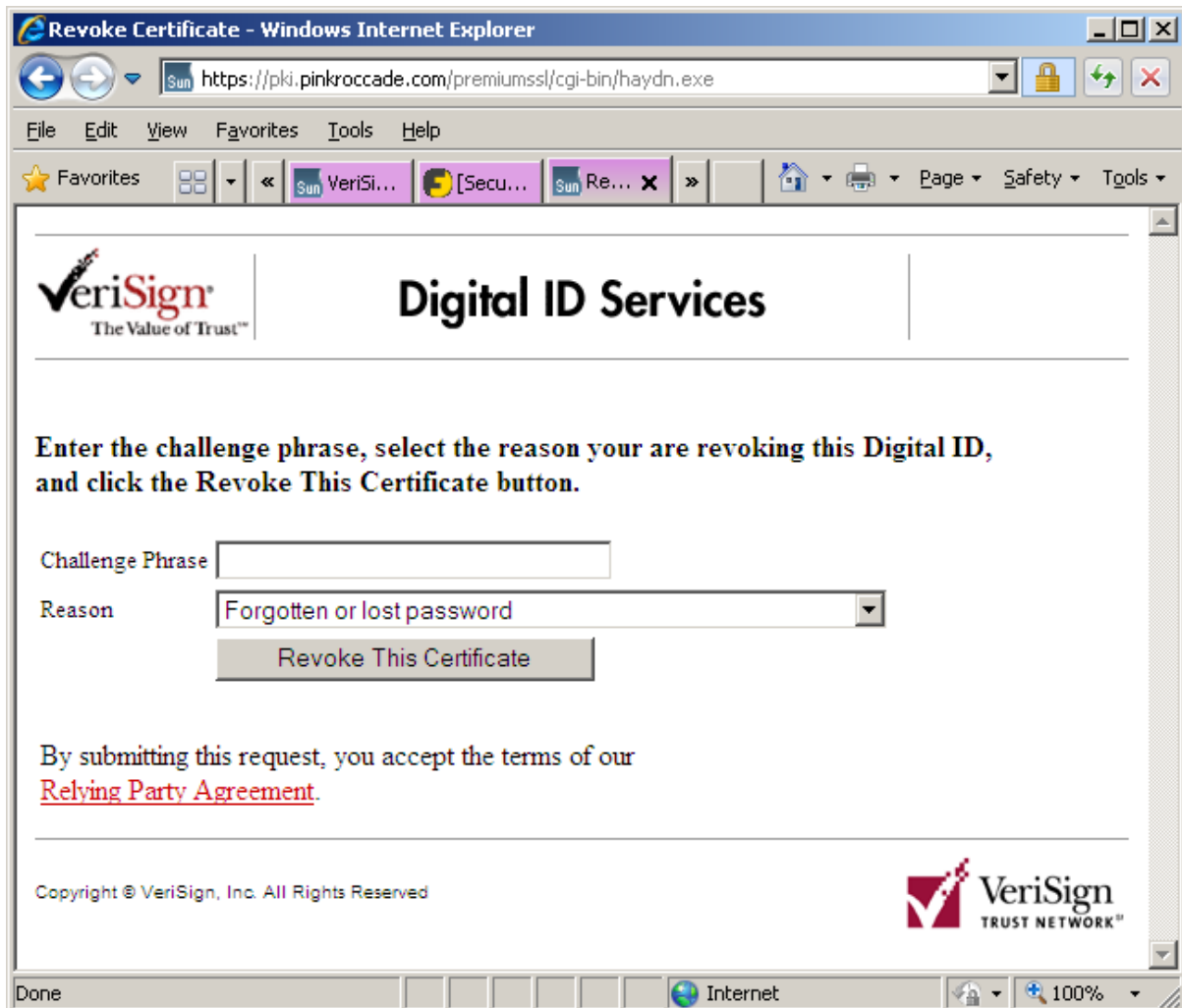
If this is the correct Digital ID, you can now choose to **revoke**, **replace**, **renew**, **set preferences** or **enroll for the additional Digital ID**.

Name	WWW.VERISIGN.COM
Status	Valid
Validity	May 26, 2010 - May 25, 2012
Class	Digital ID Class 3 - VeriSign Extended Validation Global Server Two Year
Subject	Jurisdiction Country = US Jurisdiction State = Delaware Business Category = V1.0, Clause 5.(b) Serial Number = 2497886 Country = US Postal Code = 94043 State = California Locality = Mountain View Street Address = 487 East Middlefield Road Organization = VeriSign, Inc. Organizational Unit = Production Security Services Common Name = www.verisign.com
Serial Number	53d2bef924a7245e83ca01e46caa2477
Issuer Digest	ced48c4d9e3e74b4e182f02208bae83a

[Revoke](#) [Replace](#) [Renew](#) [Set Preferences](#) [Additional Server ID](#)

By submitting this request, you accept the terms of our

The revoke function appears to be able to revoke any VeriSign certificate, if it can be provided with the correct challenge password/passphrase that was used during certificate enrolment.



[It is unknown at this time if the password can be simply brute-forced, or if the correct password is entered that the certificate is in fact revoked, or if that initiates an approval request to the MPKI administrator.]

Discovery

The vulnerability(s) was discovered initially from searching for information on VeriSign's MPKI system. A Google search for the phrase:

"Enrollment Services" verisign

Returns a number of results from the domain '*certificatemanager.verisign.com*', all of which when clicked login to a number of VeriSign customer accounts including Bank Of America, Yale University, Berkeley University and more.

Extending the search to the phrase:

"jur_hash"

As used in the VeriSign URL shows more results.

In addition, a search of the popular bookmarking site Delicious.com for the title of the VeriSign enrolment page ("Enrollment Services") displays a result that actually logs into the Production Services account of VeriSign themselves – including the ability to list every VeriSign production certificate they have issued themselves.