White Paper

# Certificates are an enterprise security asset

## Digital certificate life cycle management protects your essential assets

**Gal Alton**
Securely Ltd

Date: 01/04/2016

# Table of Contents

# Introduction

Securing data, whether at rest or in transit, has become a major concern for IT managers because of security risks originating both in house and outside. One way for organizations to increase security is by using cryptography algorithms to encrypt data. The RSA algorithm is a popular one for encryption key exchange, used during SSL sessions, and for digital signatures that provide data integrity, non-repudiation, and authentication.

Encryption keys are private and must be associated with a person or organization. Digital certificates bind the identity of the certificate holder to an encryption key.

Digital certificates play an important role in securing various types of business data and processes. They are used to secure communications and mail, in digital signatures and code signing, in client authentication, and more. Organizations can purchase certificates from public certification authorities or issue them from an internal certificate authority (internal PKI).

All certificates should be treated as an essential assets and managed similarly to other assets.

**Security Management** is a broad field of management related to asset management.

**Asset management**, broadly defined, refers to any system that monitors and maintains things of value to an entity or group. *(Wikipedia)*

All assets should be clearly identified and an inventory of all important assets drawn up and maintained.

The asset inventory should include all information necessary in order **to recover from a disaster**.

The process of compiling an inventory of assets is an important prerequisite of risk management.

*(ISO/IEC 27002)*

# Why organizations need to manage certificates as an asset

Enterprises are facing growing potential risks when using large numbers of unmanaged certificates. Some IT managers, responsible for hundreds or even thousands of certificates, still manage certificates manually, using old fashioned tools like spreadsheets. Manual management cannot provide a complete overview of enterprise risks, and it is difficult to keep track of the number and type of certificates issued, where they are installed, and what is their lifespan. The growing use of certificates makes their

**If certificates are not managed, you don't know:**

- Where they are installed
- When they expire
- Whom to alert
- What is the key length
- Who issued them
- How many certificates were issued

monitoring very time consuming and prone to human error.

> *Organizations with roughly 200 or more X.509 certificates in use that are using manual processes typically need one full-time equivalent (FTE) per year to discover and manage certificates within their organizations.* ***(Gartner, 4 November 2011)***

Using an invalid certificate can cause substantial damages, such as:

- Services outages
- Financial and business loss
- Damage to the brand name
- Exposure to cybercrime
- Data theft

If your enterprise is aware that certificates are an asset, it will monitor and manage them automatically to avoid the next disaster.

## Examples of certificate expiration incidents

### Microsoft Windows Azure Cloud Fails As SSL Certificate Expires [1]

*"Windows Azure Storage experienced a worldwide outage impacting HTTPS traffic due to an expired SSL certificate. HTTP traffic was unaffected but the event impacted a number of Windows Azure services that are dependent on Storage. We executed the repair steps to update the SSL certificate on the impacted clusters and availability was restored to >99% worldwide by 1:00 AM PST on February 23. At 8:00 PM PST on February 23, we completed the restoration effort and confirmed full availability worldwide."*


### Sage payment processor suffers 24-hour outage [2]

*"Customers logging into "secure and efficient payment service" Sage Pay this morning were served up an error message saying that the site could not be trusted, and didn't have a valid security*

[1] http://blogs.msdn.com/b/windowsazure/archive/2013/02/24/windows-azure-service-disruption-from-expired-certificate.aspx
[2] http://www.theregister.co.uk/2012/04/26/sagepay_ssl_certificate/

*certificate. Looks like someone forgot to renew the site's SSL certificate – which expired at 12:59 am this morning."*

### MI5 stinks up website with dead SSL certificate 3

*"Blighty's intelligence agency MI5 forgot to replace the expired digital certificate for its website over the weekend. The schoolboy error meant anybody trying to securely access the Security Service's site - perhaps to report suspected terrorist activity - would have been warned by their browser that the connection was untrusted. Communications would have still been encrypted if surfers chose to proceed regardless of the alert."*

### VeriSign Forgets to Renew an SSL Certificate 4

*"Though this isn't the first big company to forget to renew an SSL certificate (Google, LinkedIn, Yahoo, and the BBB have all let certificates expire), it is the first known SSL certificate provider to do so and the biggest provider of them all. SSL certificate expiration can be a problem for anyone."*

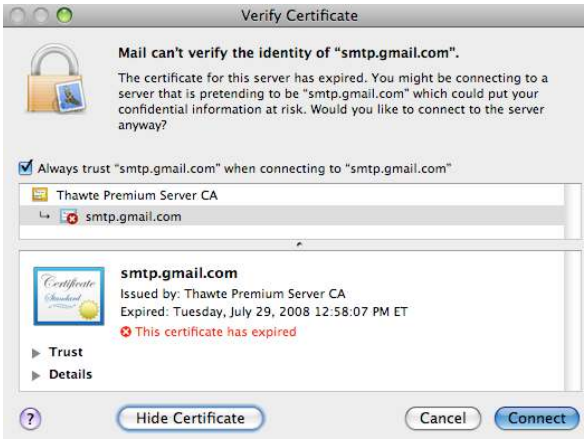
### HSBC forgets to renew its digital certificate 5

*"Online banking customers logging onto the HSBC website last week were confronted by potentially confusing warnings about a security certificate. Business banking customers logging onto ukbusiness.hsbc.com were greeted with a notice that the site couldn't be verified because its certificate had expired. HSBC said the problem persisted for about a day before it was resolved. It apologized for the glitch, which it said had no effect on either the integrity or operation of its website."*

### Google Forgets to Renew Gmail's SMTP SSL Certificate [6]

*"Google's SMTP server, smtp.gmail.com, has just expired a couple minutes ago. Here is the SSL certificate expiration notice:*

*It appears Google has forgotten to renew the certificate, even though a Google Groups post had a warning to Google that it would be expiring today."*




[3] http://www.theregister.co.uk/2012/04/16/mi5_digi_cert_snafu/
[4] http://www.sslshopper.com/article-verisign-forgets-to-renew-an-ssl-certificate.html
[5] http://www.theregister.co.uk/2008/03/10/hsbc_cert_glitch/
[6] http://www.seroundtable.com/archives/017825.html

# Key features of certificate life cycle management

*Certificate Discovery*

Several methods can be used to discover certificates

- Scanning the network to discover certificates protecting secure protocols like SSL, SSH, and SLDAP
- Importing certificates from machine key stores
- Importing certificates from workstation user stores
- Importing certificate from *".cer"* files, suitable for individual machines

## Importing certificates from a certificate authority (CA)

It is also possible to import certificates from an internal CA authority, directly from a CA database.

## Alerts and Reporting

The certificate management solution must have a variety of alert mechanisms and support the following functionality:

- Configure policy-based alerts
- Send renewal alerts, with the ability to escalate alert messages
- Use alert methods such as email, SMS, and event logs
- Issue alerts for different populations, depending on the certificate

## Renewal

- Policy-based automatic renewal of certificates
- Preparations for manual renewal, including preparing the certificate request

## Administration

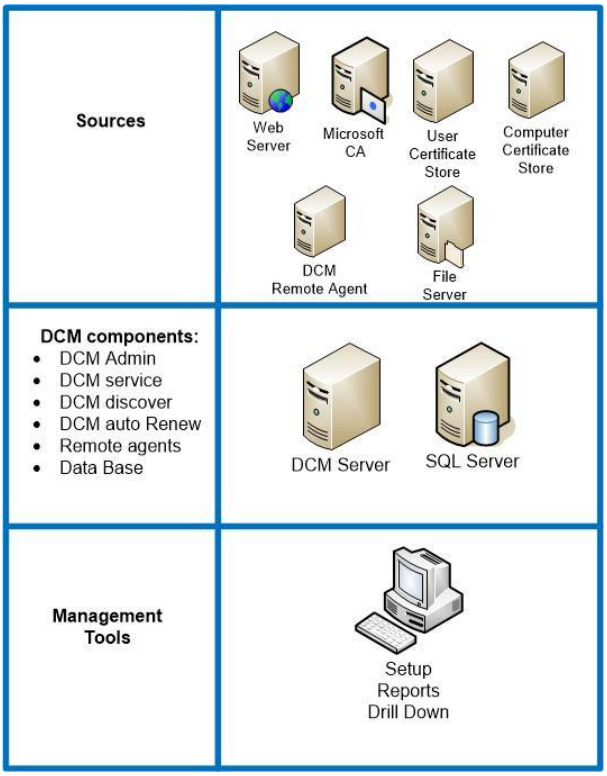
The easy-to-use GUI must provide the following functionality:

- Query tools with advanced filters to find certificate data easily
- Revoke certificate
- Reports that present important information about expiring certificates, self-signed certificates, and certificate distribution at a glance
- Convenient setup and configuration

# Digital Certificate Management (C-View)

## Description

C-View is a proven solution that helps certificate managers collect and store certificates from various sources:




- Web servers (SSL certificates)
- Microsoft internal CA database
- Certificates from the Windows computer certificate store
- Certificates collected remotely by agents
- Certificate file located in a share folder

C-View comprises of the following components:

- Discovery service
- Collection service for MS-CA
- Auto renew service
- Client agent for workstation
- PKI Monitor for Microsoft PKI
- Friendly GUI
- SQL server

C-View basic functionality are:

## Discover & Collect

Discover certificates from multiple sources: SSL certificates, Microsoft internal CA databases, *".cer"* file stored in a share folder, and computer certificate stores. Another source can be a C-View agent installed on remote networks or behind the firewall. Fetching certificates from the user certificate store requires user login. To circumvent this security requirement a thin client running on Windows platforms collects certificates from the user store and stores them in a share folder, where there are accessible to C-View for collection and management.

## Auto Renew

Define an auto renewal policy by CA's template, issued new certificate with the same subject. Auto Renew service send alerts about each renewal and saves PFX with encrypted password

## Alerts

- Certificate expiration mail and log entry
- CA server certificate expiration and half-life alert
- Microsoft CA CRL publishing and validity
- Microsoft CA server and service status

## Subscribers

- CA server administrator
- Certificate holder
- IP range managers

## Searching and Reporting

- Query MS-CA certificates
- Query revoked MS-CA  certificates
- Query discovered certificates
- Present certificate status using various types of predefined reports and diagrams
- Revoke certificates


## PKI Overview

A monitoring tool suitable for Microsoft PKI provides online status information about CA servers:

- Service health
- Server
- CA hierarchy display
- CA certificate validity
- CRL status