

The

Starter PKI Program

*Get the timesaving convenience of a *thawte* multiple digital certificate account ...*

1. Overview
2. What is the Starter PKI Program?
3. Starter PKI – the Benefits
4. How does it all Work?
5. What does it Cost?
6. Get Going Right Away
7. What Role Does *thawte* Play?
8. The Value of Authentication
9. Contact *thawte*

1. Overview

The Starter PKI program from thawte has been developed for companies with a need to secure multiple domains or host names. This guide will introduce you to the Program by explaining how it works and its benefits. We will also point you to a dummy company on our web site where you can “test drive” the Program. Finally, you’ll find out how to enroll and the costs involved. If you require further information not included in this guide, please contact the Starter PKI Business Solutions team – details available on the past page of this guide.

2. What is the Starter PKI Program?

The Starter PKI Program is a simple, pre-paid account system which makes it possible to purchase and manage renewal of multiple SSL and Code Signing certificates at discounted prices with the minimum of paperwork – perfect for organizations requiring more than FOUR digital certificates per year.

3. Starter PKI – The Benefits

The Starter PKI Program is about convenience – and setting you free to do the things you really like.

It allows you and your organization to manage your own SSL and Code Signing Certificates without the never-ending hassle of having to go through processes and red tape.

Once you've completed the initial sign-up, there is no need for day-to-day interaction with *thawte*. *thawte's* trusted root keys sign certificates, but they are authorized and approved by your own security personnel.

thawte also offers you a user-friendly on-line interface to manage your account.

You will be able to:

- Add security personnel into your account
- Prepay for discounted certificate bundles
- Utilize the management system to keep track of the certificates you have issued
- Access reports on:
 - o Cost of Certificates
 - o Date of issuance
 - o Expiry Date
- Have the ability to add new domain names, departments and subsidiary companies.

So, in summary, it makes your life easier through a number of unique benefits:

- One enrollment covers all certificates and renewals for a two-year period.
- We re-verify your company details every two years, to ensure the highest level of trust for your organization.
- Integrated, seamless, easy-to-use administration.
- Total control over requesting, editing, approving and terminating certificate requests.
- 2 – 3 hour turnaround time for all certificates.
- Full free technical support 24 hours a day, five days a week

You even get a variety of certificates from a single comprehensive console:

- SSL Web Server Certificates
- SGC SuperCerts (automatic 128-bit step-up encryption)
- Code Signing Certificates (Microsoft Authenticode, Microsoft VBA Macro Signing, Netscape Code Signing, JavaSoft)

4. How Does It All Work?

Step #1: The vetting process

When the public sees the *thawte* brand on a digital certificate, they know they are interacting with a trusted and secure digital domain. To maintain our integrity (and make sure you reap the benefits thereof), we need to vet you in a simple once-off process.

When you join the Starter PKI Program, we will request all your company documents and details – and all domain names to which you would like to issue a certificate, of course.

The reason for this is simple. Our verification team needs to check that:

- Your company is a registered company in good repute.
- You really do work at the company you claim to work at.
- Your domain names are registered to your company.
- You and your Chief Security Officer are both aware of his/her duties and responsibilities.

Step #2: Pre-validation

Once the account is approved certificate requests are matched against all your pre approved company and domain details

As long as a SSL Certificate is for a host in one of your domains, and contains a Country, State (Province) and organization name that match a pre-verified set, you are free to approve the certificate and have it signed by *thawte* immediately.

In other words, you will be able to issue certificates to all these domains without any further interaction with *thawte*.

Step #3: Setting up the test drive

The *thawte* Starter-PKI Program puts you in the driver's seat, allowing you to manage your own certificates.

But we don't expect you to know all the gears and levers from the word go. To help you familiarize yourself with your live management interface, we created a "test-drive" environment. This enables you to request certificates as well as edit, approve and terminate bogus certificate requests – all within the safe confines of our learning center.

In order to experiment, fiddle and play with the system, we have created a dummy company called ACME, which works just like the real thing.

Simply go to ...

<http://www.thawte.com/ucgi/gothawte.cgi?a=w47100166367053000>

... and start driving!

Step #4: Learning Online

Now, you can test all the things you are able to do inside your own company structure. For example:

- To request a certificate, log in to your PKI account here:
<http://www.thawte.com/spki/index.html>
- Once you are happy that everything is correct, approve the certificate. If you notice an error (for instance, a spelling error in your company name) you can choose to edit the certificate details before you approve it. If you notice that someone from your company who shouldn't be requesting a certificate has put in a request, you can terminate that request
- Adding domain names to your account is just as easy. Click on "Domain Manager" and enter the information. Your new account details will automatically be sent to your thawte Support Manager, who will confirm that the domains in fact belong to you. As soon as this has been approved, you will immediately be able to issue certificates to your new domains

All this functionality will be available in your real SPKI account

5. What does it Cost?

The *thawte* Starter PKI Program is highly adaptable – even when it comes to price. Participants are eligible for discounts of 25% and up on all *thawte* digital certificates. Please contact our Starter PKI Business Solutions team for more information.

6. Get Going Right Away

If you want the trust, security and convenience of *thawte's* Starter PKI Program to start working for you right away, we will be delighted to serve you at: <http://www.thawte.com/spki/index.html>

7. What Role Does *thawte* Play?

thawte Technologies is a Certification Authority (CA) which issues SSL Web Server Certificates and 128-bit SuperCerts to organizations and individuals worldwide. *thawte* verifies that the Organization ordering the certificate is a registered organization and that the person in the organization who ordered the certificate is authorized to do so.

thawte also checks that the organization in question owns the relevant domain. *thawte* digital certificates interoperate smoothly with the latest software from Microsoft and Netscape, so you can rest assured that your purchase of a *thawte* Web Server Certificate will give your customers confidence in your system's integrity - they will feel secure about transacting online.

8. The Value of Authentication

Information is a critical asset to your business. To ensure the integrity and safety of your information, it is important to identify with whom you are dealing, and the data you are receiving is trustworthy. Authentication can help establish trust between parties involved in all types of transactions by addressing a unique set of security issues including:

Spoofting:

The low cost of website design and the ease with which existing pages can be copied makes it all too easy to create illegitimate websites that appear to be published by established organizations. In fact, con artists have illegally obtained credit card numbers by setting up professional looking storefronts that mimic legitimate businesses.

Unauthorized Action:

A competitor or disgruntled customer can alter your website so that it malfunctions or refuses to service potential clients.

Unauthorized Disclosure:

When transaction information is transmitted "in the clear", hackers can intercept the transmissions to obtain sensitive information from your customers.

Data Alteration:

The content of a transaction can be intercepted and altered en route, either maliciously or accidentally. User names, credit card numbers and currency amounts sent "in the clear" are all vulnerable to alteration.

9. Contact *thawte*

Should you have any further questions regarding the content of this guide or *thawte* products and services, please contact a Sales Advisor:

E-Mail: spkisaales@thawte.com

Telephone: +27 21 937 8977

Fax: +27 21 937 8967