MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Matrix42 Silverback

Apple DEP Enrolment Guide

Version 0.0.1

9. December 2015

Copyright © 2000 - 2014 Matrix42 AG

This documentation is copyright protected. All rights are reserved by Matrix42 AG.

Any other use, in particular the disclosure to third parties, storage in a data system, dissemination, processing, presentation, performance and demonstration are prohibited. This applies to the entire document, as well as parts thereof.

Subject to change. Reprint, also in excerpts, is permitted only with the written consent of Matrix42 AG.

The software described in this document is subject to a permanent development due to which there may be differences in the documentation and the actual software. This documentation is not entitled to the actual functionality of the software.

Apple and **Mac OS X** are registered trademarks of Apple Inc.
Citrix® software or **Citrix® server** are Trademarks and Registered Trademarks of Citrix Systems, Inc. in the United States and other countries.
cygwin is copyrighted by Red Hat Inc. 1996-2003.
expat is copyrighted by Thai Open Source Software Center Ltd.
gSOAP is copyrighted by Robert A. van Engelen, Genivia, Inc. All rights reserved.
Iconv is copyrighted by 1999-2003 Free Software Foundation, Inc.
Iperf is copyrighted by the University of Illinois, except for the gnu_getopt.c, gnu_getopt_long.c, gnu_getopt.h files, and inet_aton.c, which are under the GNU General Public License.
Libmspack (C) 2003-2004 by Stuart Caie <kyzer@4u.net>.
OpenSSL This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
PuTTY is copyrighted by Simon Tatham. Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, and CORE SDI S.A.
RSA Data Security, Inc. MD5 Message-Digest Algorithm is copyrighted by RSA Data Security Inc. Created 1991. All rights reserved.
rsync is an open source utility that provides fast incremental file transfer. rsync is freely available under the GNU General Public License version 2.
runcontrol The Initial Developer of the Original Code is James Clark. Portions created by James Clark are Copyright (c) 1998 James Clark. All rights reserved.
SNMP++ Copyright (c) 1996 Hewlett-Packard Company.
VMware, the **VMware "boxes" logo and design, Virtual SMP, VMotion vSphere, vSphere Hypervisor (ESXi), ESX, View, ThinApp, vCenter** and **vCloud** are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
Windows, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and **Windows Server 2012** are registered trademarks of Microsoft Corporation.

Others, at this point not explicitly listed, company, brand and product names are trademarks or registered trademarks of their respective owners and are subject to trademark protection.

Contents

1. Introduction 4
2. Prerequisites 5
2.1. Enrolment into Apple's DEP Program 5
2.2. Mac Computer with Latest OSX 5
3. Create a Unique SSL Keypair 6
3.1. Create a Unique Certificate 6
3.2. Exporting your Certificate 7
4. Extracting both Public and Private Keys 8
5. Decrypting your DEP Token 9

Apple DEP Enrolment Guide

1. Introduction

The Device Enrolment Program offered by Apple provides IT Administrators an easy way to ‘fast track’ their device rollout of Corporate owned Apple Devices. This document will help guide you through how to create your DEP Token to begin enrolling your devices into Silverback once Apple have approved your DEP Account.

2. Prerequisites

You will need to ensure you have completed your enrolment into Apple's DEP Program and that you have access to a Apple Mac Computer running the latest Version of OSX.

2.1. Enrolment into Apple's DEP Program

To begin the process of enrolling into Apple's DEP Program visit the https://deploy.apple.com website and provide the following information:

- Business or Institution Phone Number and Email Address
  - The Email Address provided must be tied to your corporate domain. Consumer Email Addresses will not be accepted (Gmail/Hotmail/Yahoo! Etc.).
- Verification Contact
  - Contact Information for an individual who can confirm you have the legal authority to bind your organization to the Device Enrolment Program.
- Business or Institution Information
  - Address Information
  - Dun & Bradstreet Number (DUNS)
- Apple Customer Number
  - This is the Account Number assigned to your business or institution when you purchase Apple Hardware or Software directly from Apple.

Submit this information to Apple and you will be contacted for additional information or when the enrolment process is completed.

2.2. Mac Computer with Latest OSX

The Process of creating the DEP Token requires access to the Keychain App and Terminal with OpenSSL, which are tools built into OSX.

3. Create a Unique SSL Keypair

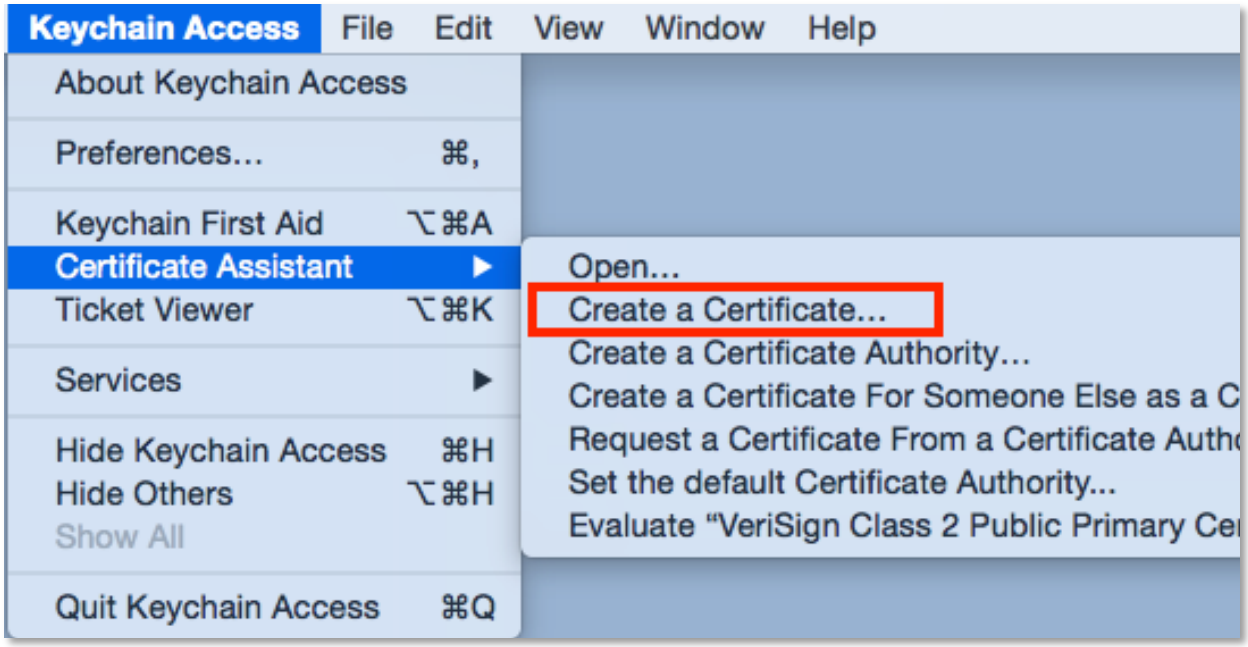
As part of the DEP Creation Process the Customer will be providing a Public Certificate to Apple which will turn into our DEP Token.

To Start This Process we will be creating a Unique SSL Keypair using Keychain in Mac OSX.

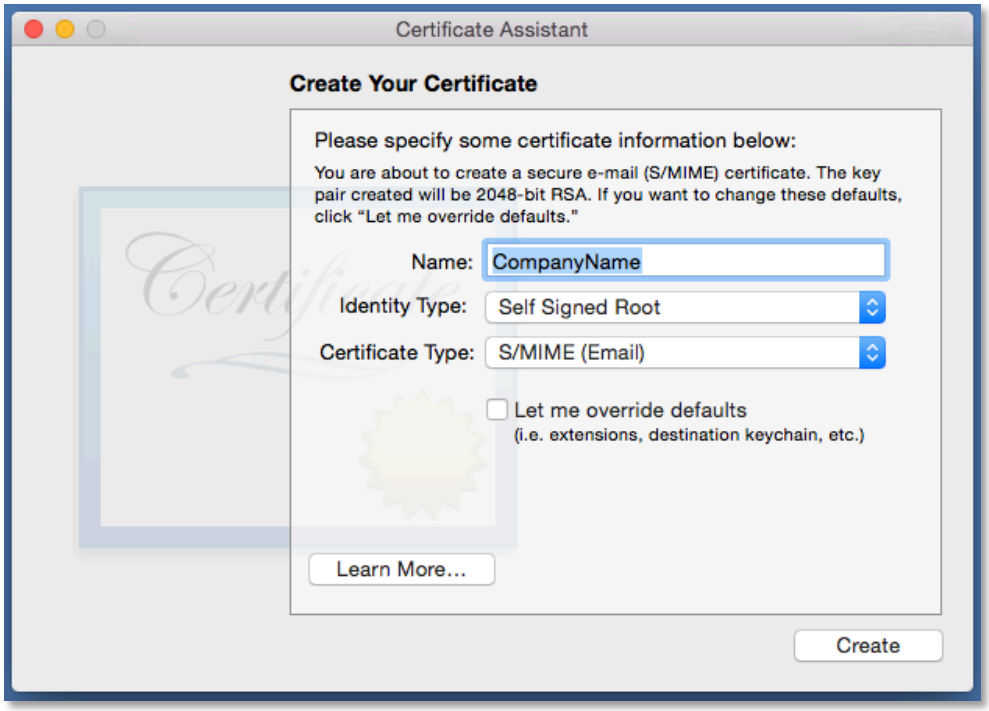
3.1. Create a Unique Certificate

Log into your Mac Computer, and open the Keychain Application. This can be done by going to Launchpad and typing in 'Keychain'.

Once open, visit the Keychain Access Menu and from the Certificate Assistant menu choose the Create a Certificate option.



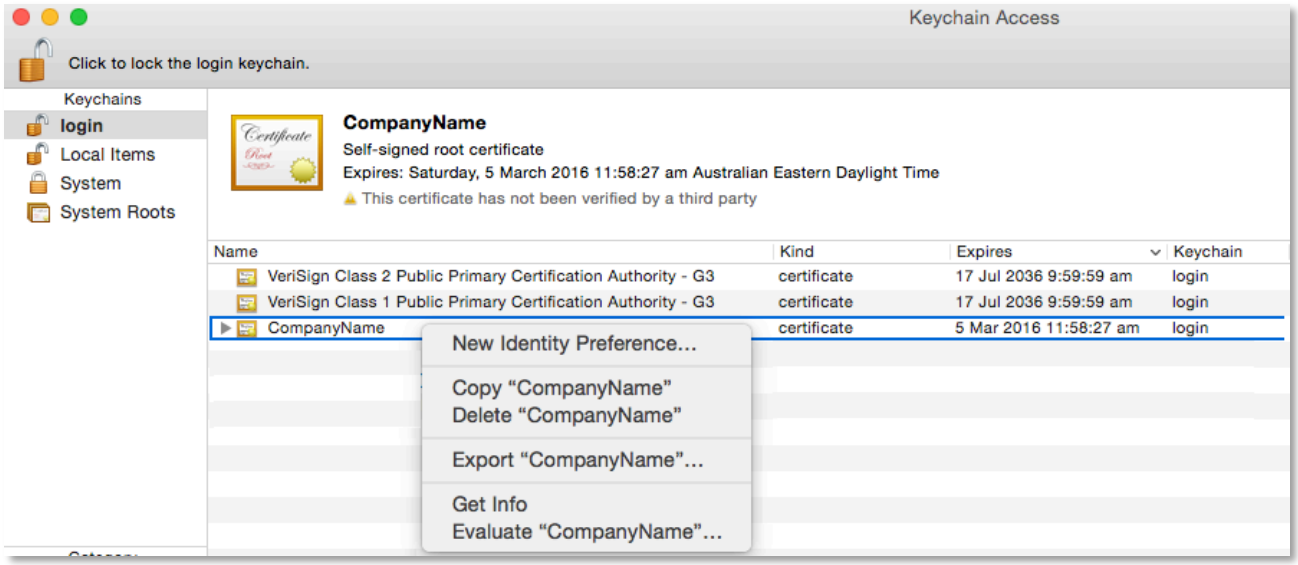
In the ‘Certificate Assistant’ wizard that appears, Enter in the Company Name and ensure that the Certificate Type is set to S/MIME (Email) then click the Create button.



3.2. Exporting your Certificate

Once the ‘Certificate Assistant’ has completed your Certificate, Right-Click on your Company Certificate and Export it to a location on your computer as CompanyName.p12.

NOTE: We will be using this file in the next section of the document.



4. Extracting both Public and Private Keys

Using the Terminal Application within Mac OSX, navigate to the directory that contains your Exported Certificate from Section 3.2 and execute the following command:

```
openssl pkcs12 -in CompanyName.p12  -out CompanyName.pem –nodes
```

NOTE: You will be asked for the Export Password you set during Section 3.2.

The CompanyName.pem file that is created can be opened in a standard Text Editor and will look similar to the display below.

Save the Text in Green in a separate file named *CompanyPublic.key*

Save the Text in Blue in a separate file named *CompanyPrivate.key.*


```
Bag Attributes
    friendlyName: CompanyName
    localKeyID: 6D 41 81 8D C1 C4 FC 7B C1 4C 24 E0 97 DA 2C 77 DB 9C B5 F1
subject=/CN=CompanyName/C=AU
issuer=/CN=CompanyName/C=AU
-----BEGIN CERTIFICATE-----
MIIC6TCCAdGgAwIBAgIBATALBgkqhkiG9w0BAQswIzEUMBIGA1UEAwwLQ29tcGFu
eU5hbWUxCzAJBgNVBAYTAkFVMB4XDTE1MDMwNjAwNTgyN1oXDTE2MDMwNTAwNTgy
gVglG0SWc/QzJflcyRXUEW4rFJ9joEBnyeN4jibKPWvB5RKqh5lly/5H5nljp+6
pX7EwM63aVmsd5MxEVMT8isAXDVi+DWkzBHc4fQ=
-----END CERTIFICATE-----
Bag Attributes
    friendlyName: CompanyName
    localKeyID: 6D 41 81 8D C1 C4 FC 7B C1 4C 24 E0 97 DA 2C 77 DB 9C B5 F1
Key Attributes: <No Attributes>
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA7marEWleBfTWC1nF8uf2PRputQJeAEnyZfP/D0TO22W2TIzT
jd4NWETfehzq3e/W5WcjQ79NNNAq9KwxsPPNq5OEJFzDEgdZGV0enHaEfi4i7YSK
j9BSH3ECgYAYcXHzjg5tcTQVaHfkI8X/hd9w56iSJC3gEdEC7WnGOiSeqhp/ZeP8
iXZVp66EuajK4QwMYHE2lpzqxTAieWYYmA3sic+uLU3zBdjjBNmWKcUE/soqzel9
ySfNSOx+SHxE+fCOw19udZapVwHyt93lehjkImMJqhgEJRd6QMcIwg==
-----END RSA PRIVATE KEY-----
```


Send the CompanyPublic.key file to your customer, as this is what they need to submit to Apple. They will be provided with a P7M file that is needed for the following section.

5. Decrypting your DEP Token

Using the P7M File returned and the CompanyPrivate.key file created in Section 4, we can decrypt our DEP Token for Device Enrolment.

Copy your P7M file into the same directory as your CompanyPrivate.key file, then using Terminal execute the following command:

```
openssl smime –decrypt –in encryptedToke.p7m –inkey CompanyPrivate.key > DEPToken.json
```

Finally, we now need to remove OpenSSL Header Information from the DEPToken.json file before it can be uploaded into Silverback.

BEFORE

Content-Type: text/plain;charset=UTF-8
Content-Transfer-Encoding: 7bit

-----BEGIN MESSAGE-----
{"consumer_key":"CK_e568c2688a621bb0400247fd7cf05ef19be58cba1cb26a0ec35c","consumer_secret":"CS_0a9a300f00","access_token":"AT_O8190583125113472c01f6cO1425861731668","access_secret":"AS_968be8277c0694d27df040d4765","access_token_expiry":"2016-03-08T00:42:11Z"}
-----END MESSAGE-----

AFTER

{"consumer_key":"CK_e568c2688a621bb0400247fd7cf05ef19be58cba1cb26a0ec35c","consumer_secret":"CS_0a9a300f00","access_token":"AT_O8190583125113472c01f6cO1425861731668","access_secret":"AS_968be8277c0694d27df040d4765","access_token_expiry":"2016-03-08T00:42:11Z"}