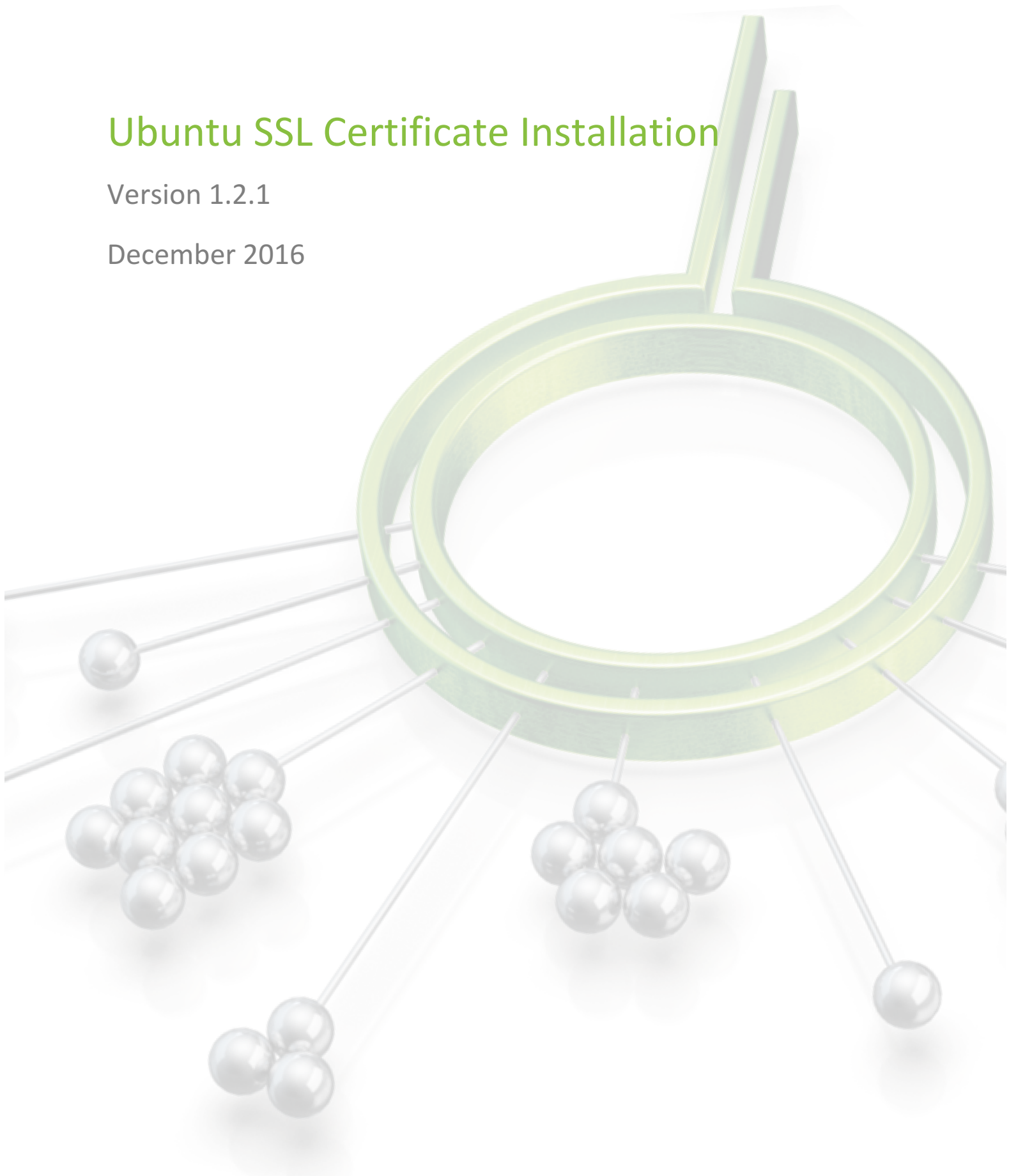# Ubuntu SSL Certificate Installation

Version 1.2.1

December 2016

Introduction

The purpose of this document is to describe how to get the Cato SSL Certificate and deploy it locally on **Ubuntu**.

Overview

Installing the Cato Networks Certificate, and adding it as a trusted application, allows users to benefit from Cato security services and reduce the extra system notifications produced by the following instances:

- **Block HTTPS traffic:** If SSL traffic is being blocked (i.e. URL filtering, Internet Firewall rules), Cato Network Certificate allows access to blocked pages.
- **TLS inspection on client's traffic:** If TLS is enabled, the web browser prompts that the connection is not private (as expected certificate was supposed to be issued by the target). The Cato Network Certificate bypasses this notification.

Installing on Ubuntu

1. Open the relevant PEM file
2. The following popup opens. Press **Import**
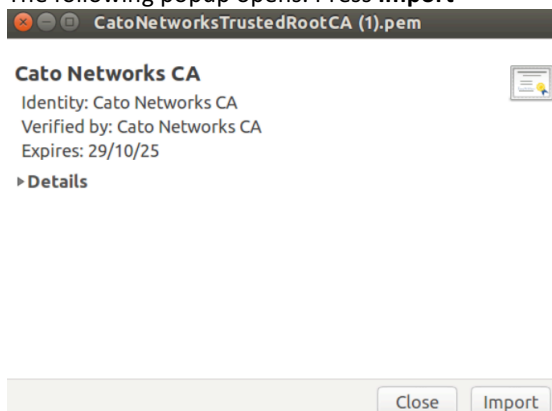
3. Upon successful installtion, press Done.

Installing on FireFox

Since Firefox does not use the operating system's certificate store by default, please follow the below steps for more

1. Access the Import certificate screen (under Preferences->Advanced)
2. Click "**View Certificates**"
3. Click "**Import**"
4. Navigate to where you stored the certificate and click "**Open**"
5. Click "**Import".** The downloading Certificate dialog displays.
   a. Select "**Trust this CA to identify websites**" and click **OK**

Additional resources

In case of issues please contact Cato Network's support at support@catonetworks.com