ORACLE

Technical Brief

Oracle Cloud Infrastructure (OCI) Certificates

Managing private Certificate Authorities and
SSL/TLS certificates

February 2022, Version1.0
Copyright © 2022, Oracle and/or its affiliates

ORACLE

Purpose statement

This document provides an overview of features and enhancements included in the release of Oracle Cloud Infrastructure Certificates (OCI Certificates). It is intended solely to help you assess the business benefits of using OCI Certificates and to plan your IT professional projects.

Disclaimer

This document in any form, software, or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

ORACLE

Introduction

Oracle Cloud Infrastructure (OCI) Certificates (https://www.oracle.com/security/cloud-security/ssl-tls-certificates/) is a service for creating and managing Transport Layer Security (TLS) / Secure Socket Layer (SSL) certificates. The service enables organizations to create private Certificate Authorities (CA) hierarchies and TLS certificates that can be integrated easily with OCI services such as OCI Load Balancing (https://www.oracle.com/cloud/networking/load-balancing/) and OCI API Gateway (https://www.oracle.com/cloud-native/api-management/). As a result, OCI Certificates service can deploy and renew certificates automatically in the customer tenancy.
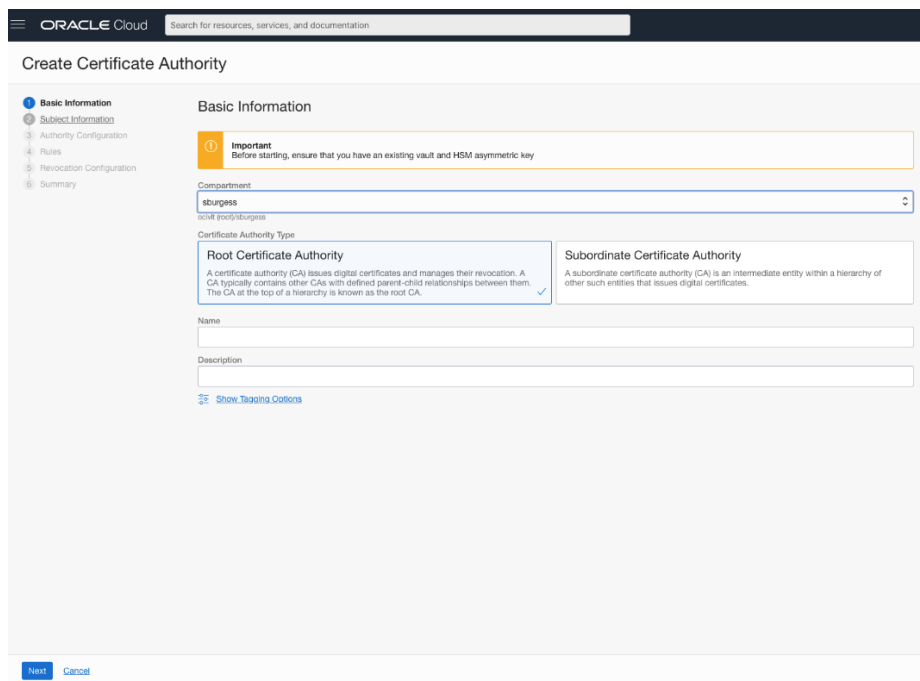

Figure 1 – Create Certificate Authority

OCI Certificates

To help enforce privacy and data security, computer systems (e.g., servers, web applications, email, etc.) should use TLS to encrypt the communication and flow of information. Enabling TLS requires the use of a TLS certificate, also known as an SSL certificate. Unfortunately, managing these certificates can be a confusing and daunting, yet critical task. OCI Certificates is a cloud-based X.509 certificate service designed to help streamline and ease the management of these certificates.

Every certificate the customer manages must have a Public Key Infrastructure (PKI) private key. Many corporations do not have the knowledge and discipline to manage PKI keys. Many third-party solutions

"A certificate will get renewed or will expire according to the rules that we set up through the OCI Console. This is something that before, and without the OCI Certificate service, you have to handle manually, with the risk of human error and so on. It is really helpful in being compliant with the regulators, external and internal auditors, and it makes OCI easier to use."

Pietro Lascari

Delivery Manager, ALEF

ORACLE

such as OCI Vault (https://www.oracle.com/security/cloud-security/key-management/) were created to solve these problems for the customers. The private key is used in the process of creating a Certificate Signing Request (CSR), and that CSR can then be sent to a CA to be signed. The CA must verify the customer owns the domain requested to protect the certificate. Once the CA signs the certificate, the certificate can be installed on the servers to enable encrypted TLS communication.

To avoid service disruptions, the expiration date of the certificate must be monitored and renewed before it expires. With a handful of certificates, the process may be cumbersome and time-consuming; however, for large companies that use thousands of certificates, managing those certificates can become a full-time job for multiple people.

The biggest pain points related to TLS certificates are 1) managing private keys and the certificates created using them, 2) keeping track of certificate inventory, and 3) renewing certificates before they expire to prevent service outages.

Managing Certificates

OCI Certificates enables customers to create self-signed private root CAs, private CA hierarchies and private certificates. After creating the CA hierarchy and certificates, the service can deploy the certificates automatically to cloud services such as Load Balancer as a Service (LBaaS) or API Gateway in the customer's OCI tenancy. OCI Certificates will then monitor the expiration date and renewal rules for the certificate and renew the certificate automatically. This automation saves time and money, because IT professionals are no longer required to manage the organization's certificates. The certificate renewal rules help prevent service disruptions, which are commonly caused by expired certificates.

For the best security posture, an HSM (Hardware Security Module) key is required to create a CA. OCI Vault service integrates with OCI Certificates to easily use the customer's private key to create a CA. OCI Certificates will never have direct access to the private key, nor will it retain copies. The service supports Federal Information Processing Standards 140 (FIPS 140) compliant RSA and ECDSA algorithms for creating a CA. Oracle's validation approach on FIPS can be found here: https://www.oracle.com/corporate/security-practices/assurance/development/external-security-evaluations/fips/.

Customers can create certificates in several categories:

- An *internally managed* certificate lives completely in the service ecosystem and can be fully automated for deployments and renewals.

- *Managed externally* enables the customer to manage their private keys or use other third-party solutions to manage them. Customer must create a Certificate Signing Request (CSR) and submit it to OCI Certificates for one of the CAs to sign.

ORACLE

- Finally, the service supports *imported* certificates, or *bring your own certificates,* in the event the customer has an existing certificate, or are required to use certificates from a specific vendor.

OCI Certificates has four predefined *profiles* to easily create certificates for particular use cases.

1. A **TLS Server or Client** is conveniently used in mTLS (mutual TLS) communications.

2. The **TLS Server** profile is specific to certificates that will be installed for the server role.

3. The **TLS Client** is for certificates that are installed on the client role machines.

4. The **TLS Code Signing** profile for certificates is used to sign applications and deployments. One use case is customers can use a code signing certificate is to sign their applications to be installed on their employees' devices. Since the devices are in the company's control, the root CAs public certificate is installed on the device to trust the application bundle.

For mTLS use cases, the customer can install a **CA Bundle** which is the root and subordinate CA certificates in a file, on the integrated resource. When a client certificate is presented, it is checked against the CA Bundle to ensure the client certificate was signed by one of the trusted CAs in the bundle. If the certificate is trusted, the connection is accepted. Otherwise, the connection is rejected.

OCI Certificates retains certificate versions, and it maintains the state of the certificate: current, previous, pending, or revoke. The *current* state indicates that the certificate is deployed on the resource(s), while all older versions of the certificate are marked as *previous*. A state of p*ending* is a flag that, although the certificate is newer than the *current* certificate, it has not yet been deployed to production. A stage of r*evoke* indicates the certificate has been added to the Certificate Revocation List (CRL) and should no longer be trusted.

Versions

Version Number	Stage	Serial Number	Revocation Reason	Not Valid Before	Not Valid After	Created	
3 *(latest)*	🟡 Pending	...550556	-	Tue, Sep 21, 2021, 17:44:44 UTC	Tue, Dec 21, 2021, 00:00:00 UTC	Tue, Sep 21, 2021, 17:44:44 UTC	⋮
2	🟢 Current	...230144	-	Tue, Sep 14, 2021, 13:50:16 UTC	Tue, Dec 14, 2021, 00:00:00 UTC	Tue, Sep 14, 2021, 13:50:17 UTC	⋮
1	⚪ Previous	...536212	-	Tue, Jul 13, 2021, 23:53:39 UTC	Wed, Jul 13, 2022, 00:00:00 UTC	Tue, Jul 13, 2021, 23:53:40 UTC	⋮

Showing 3 Items ‹ Page 1 ›

Figure 2 - The various stages of the lifecycle of the certificate

Once the customer has configured the integrated resource with a TLS certificate from the OCI Certificates service, an *association* is made with the resource. This association will help prevent an accidental deletion of the certificate. To delete the certificate, the customer must remove the association intentionally, and only then can the certificate be deleted safely. This association will help keep the customer's private key, certificate, and

ORACLE

service using the certificate safe from operator error that may result in a service outage.

Conclusion

The use of OCI Certificates helps ensure that the communication with cloud resources is encrypted and secured at no additional cost. OCI Certificates addresses the error-prone and time-consuming process of TLS certificate configuration, renewals, and deployments. With OCI Certificates, customers can create a CA hierarchy and certificates quickly that can be deployed automatically to integrated resources. Automating the processes to deploy, monitor, and renew certificates helps avoid service disruptions that result from expired certificates. OCI Certificates enable the customer to configure it once, and more efficiently and effectively manage TLS certificates. Finally, OCI Certificates reduces the cost and the worry of encrypted connections, enabling businesses to focus on more important goals.

Additional Resources

- More information about OCI Certificates: https://www.oracle.com/security/cloud-security/ssl-tls-certificates/
- Frequently Asked Questions about OCI Certificates: https://www.oracle.com/security/cloud-security/ssl-tls-certificates/faq/
- Documentation about OCI Certificates: https://docs.oracle.com/en-us/iaas/Content/certificates/home.htm

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

🅱 blogs.oracle.com   🅵 facebook.com/oracle   🐦 twitter.com/oracle

ORACLE