

## Online certificate distribution for STSAFE-A products

### Introduction

STMicroelectronics offers the Online Certificate Distribution (OCD) service to provide customers with their object certificates to:

- Prevent customers from reading certificates/UID for each of the IoT devices.
- Provide customers with a fast method to enroll IoT devices to cloud networks.
- Ease the journey of the customers willing to use the STSAFE-A UID and Root of Trust (RoT) with a different Certificate Authority (CA) than STMicroelectronics.

The OCD service offers the following features:

- Reel of the secure elements preprovisioned with the OCD personalization profile.
- A zip file containing all certificates of the reel ordered by the customer.
- Secure access to myST platform: certificates and documentation related to the OCD service are accessible through the customer secure account on the MyST platform.

This application note applies to the STSAFE-A110 and STSAFE-A120 devices.

### The STSAFE-A solution

The STSAFE-A is a highly secure solution that acts as a secure element providing authentication and secure data management services to a local or remote host. It consists of a full turnkey solution with a secure operating system on the latest generation of secure microcontrollers.

The STSAFE-A can be integrated into internet of things (IoT) devices, smart home, smart city and industrial applications, consumer electronics devices, consumables, and accessories.

Figure 1. OCD



DT74574

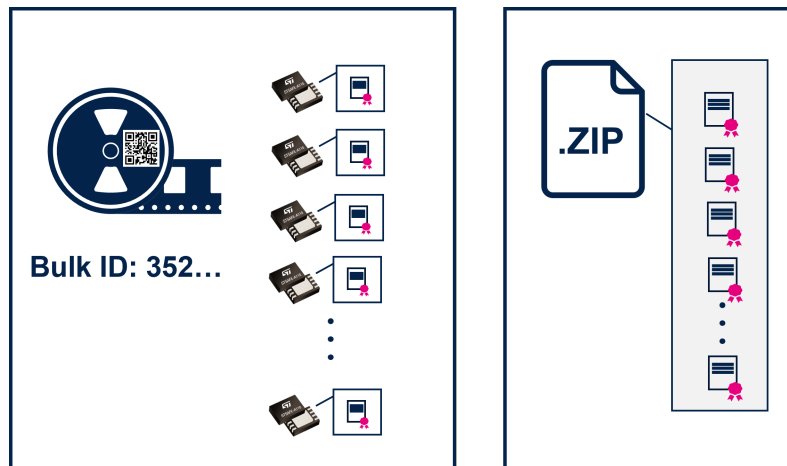
# 1 Online certificate distribution

## 1.1 OCD overview

Two different ways are available to access the OCD service:

- By scanning the QR code located on the reel as well as on its packaging, and by logging on to MyST secure account.
- By going on the [certificate claim page](#) and entering the bulk ID.

**Figure 2. STSAFE-A certificate delivery schemes**



DT74510V1

Customers can then access bulk certificates and download all documents related to the OCD service.

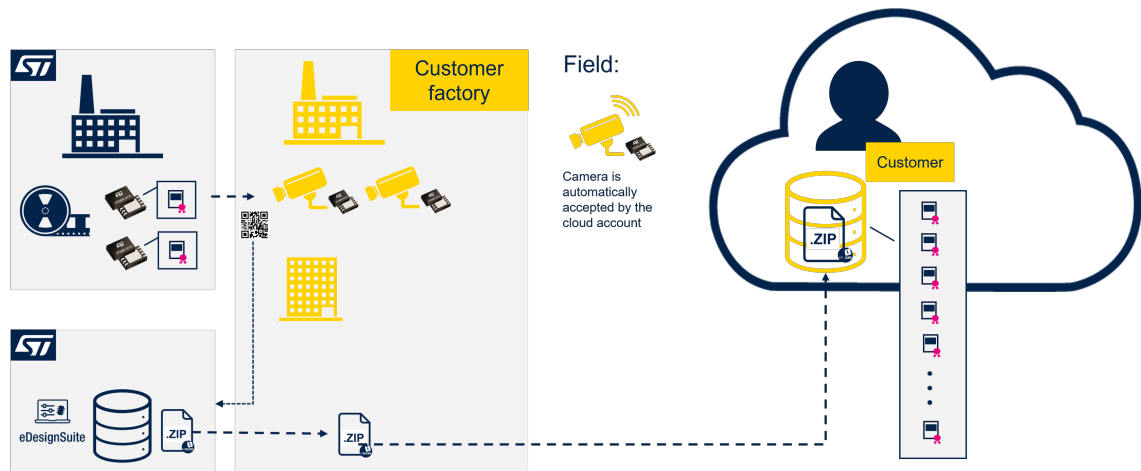
## 1.2 How to benefit from the OCD service to enroll the devices

The security of the cloud-based services relies on the strict authentication of the connected objects.

A cloud account containing the X.509 certificates of the objects can strictly authenticate the connected devices where the STSAFE-A is mounted. Each device can be enrolled one by one, by registering its X.509 certificate.

This authentication requires that the objects are enrolled to the targeted services before they are put on the market by the OEM. The OCD service enables each connected object to enrol one at a time, without any certificate query needed on the object.

**Figure 3. Device enrollment**



DT74511V1

### Enrolling each single device to a cloud account

STSAFE-A includes an X.509 certificate, that contains a unique ID and a key, to be able to authenticate. A cloud account containing the X.509 certificate can use it to strictly authenticate the connected device where the is mounted. Each device can be enrolled to a cloud account by registering the X.509 certificate to the cloud account.

## 1.3 How to assign a new certificate to a device using the OCD service with an external certificate

The STSAFE-A with OCD profile relies on the same two-level Public Key Infrastructure (PKI) hierarchy. STMicroelectronics is acting as a CA.

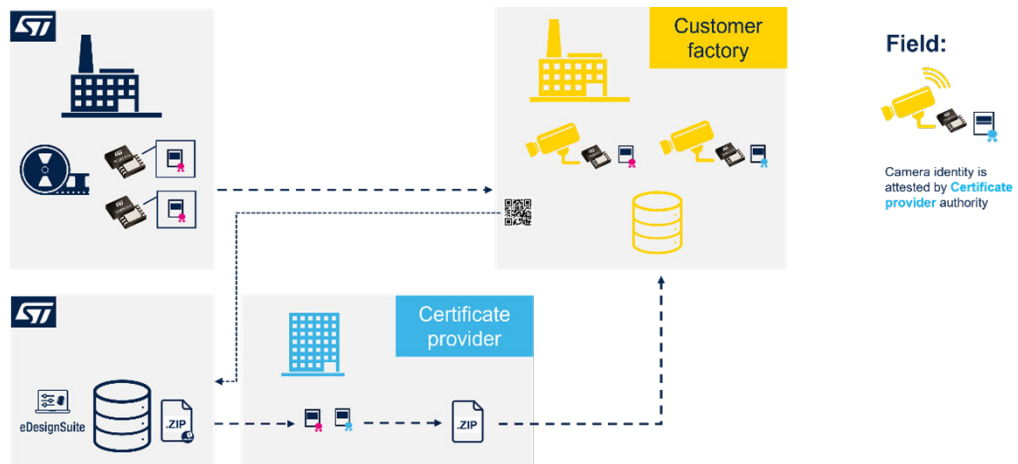
Each contains a specific private key and a leaf certificate containing a serial number and a public key corresponding to the private key. This leaf certificate is signed by STMicroelectronics CA. Each and its X.509 leaf certificate is attestable using the STMicroelectronics root CA certificate.

Customers are given the possibility to assign a new external RoT without breaking the initial STMicroelectronics RoT.

Device makers might need to build X.509 certificates that are dedicated to certain objects, and that are certified by specific certificate authorities. The OCD service eases the creation of these specific certificates:

- The OCD ensures the preloading of the X.509 certificates with the OCD personalization.
- The initial X.509 certificate can be transferred to the object certificate provider.
- The object certificate provider can extract the UIDs and the public key to reuse them into the newly created X.509 certificates of the object.
- The object certificate provider can sign the X.509 object certificates on its own, or have them signed by another CA.
- On the manufacturing side, the device maker can load into the object the new X.509 certificate of the object, whose UID matches with the initial X.509 certificate.

**Figure 4. Certificate assignment**



DTT4519V1

## Revision history

**Table 1. Document revision history**

Date	Revision	Changes
22-Oct-2024	1	Initial release.

---

## Contents

<b>1</b>	<b>Online certificate distribution</b>	<b>2</b>
1.1	OCD overview	2
1.2	How to benefit from the OCD service to enroll the devices	2
1.3	How to assign a new certificate to a device using the OCD service with an external certificate	3
	<b>Revision history</b>	<b>4</b>
	<b>List of tables</b>	<b>6</b>
	<b>List of figures</b>	<b>7</b>

## List of tables

**Table 1.** Document revision history ..... 4

## List of figures

<b>Figure 1.</b>	OCD . . . . .	1
<b>Figure 2.</b>	STSAFE-A certificate delivery schemes . . . . .	2
<b>Figure 3.</b>	Device enrollment . . . . .	2
<b>Figure 4.</b>	Certificate assignment . . . . .	3

**IMPORTANT NOTICE – READ CAREFULLY**

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to [www.st.com/trademarks](http://www.st.com/trademarks). All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2024 STMicroelectronics – All rights reserved