

PROCEDIMIENTO				
PROCEDIMIENTO CONEXIÓN DESDE AGENCIA DE REGISTRO HACIA LA ECA				
Código	PRO-ECA-29	Revisión	3	Página 1 de 4

1. GESTION DEL DOCUMENTO

FIRMA		FIRMA		FIRMA	
Elaborado por		Revisado por		Aprobado por	
Nombre	Robin Caballero	Nombre	Miguel Gutierrez	Nombre	Jose Luis Moron
Cargo	Oficial Seguridad	Cargo	Operador ECA	Cargo	Gerente Digicert
Fecha	24-nov-2023	Fecha	24-nov-2023	Fecha	24-nov-2023

2. CONTROL DE CAMBIOS

2.1. CAMBIOS AL PROCEDIMIENTO

Este procedimiento será revisado al menos una vez al año, con el objetivo de incorporar los cambios derivados de los avances tecnológicos y las modificaciones en la estructura organizativa de la empresa, las regulaciones y normas externas.

2.2. DETALLE DE CAMBIOS

Revisión	Fecha	Detalle de modificaciones
0	19-may-2022	Versión inicial del documento
1	23-feb-2019	Se actualizó la configuración de conexión VPN entre oficina DIGICERT y la ECA DIGICERT. Se describió la conexión entre las ARs y la ECA DIGICERT. Se describió la interconexión de los servidores y las funciones de cada uno.
2	05-sep-2022	Se actualizo los gráficos y describió contenido el mismo. Se quitó VPN ya que FUNDEMPRESA ya no está operando.
3	24-nov-2023	Se actualizo firmantes y contenido

3. OBJETO

El objetivo de este documento es describir la conectividad de la ECA DIGICERT y las AR.

4. ALCANCE O CAMPO DE APLICACIÓN

Este procedimiento aplica a toda operativa de integración entre la Red de las Agencia de Registro y la red de la ECA DIGICERT.



PROCEDIMIENTO				
PROCEDIMIENTO CONEXIÓN DESDE AGENCIA DE REGISTRO HACIA LA ECA				
Código	PRO-ECA-29	Revisión	3	Página 2 de 4

5. DOCUMENTO DE REFERENCIA

Código	Nombre / Título
POL-ECA-01	SEGURIDAD DE LA INFORMACIÓN
DIT-ECA-03	HABILITAR ONESHOT EN LA INFRAESTRUCTURA DE LA AR

6. DEFINICIONES Y ABREVIATURAS

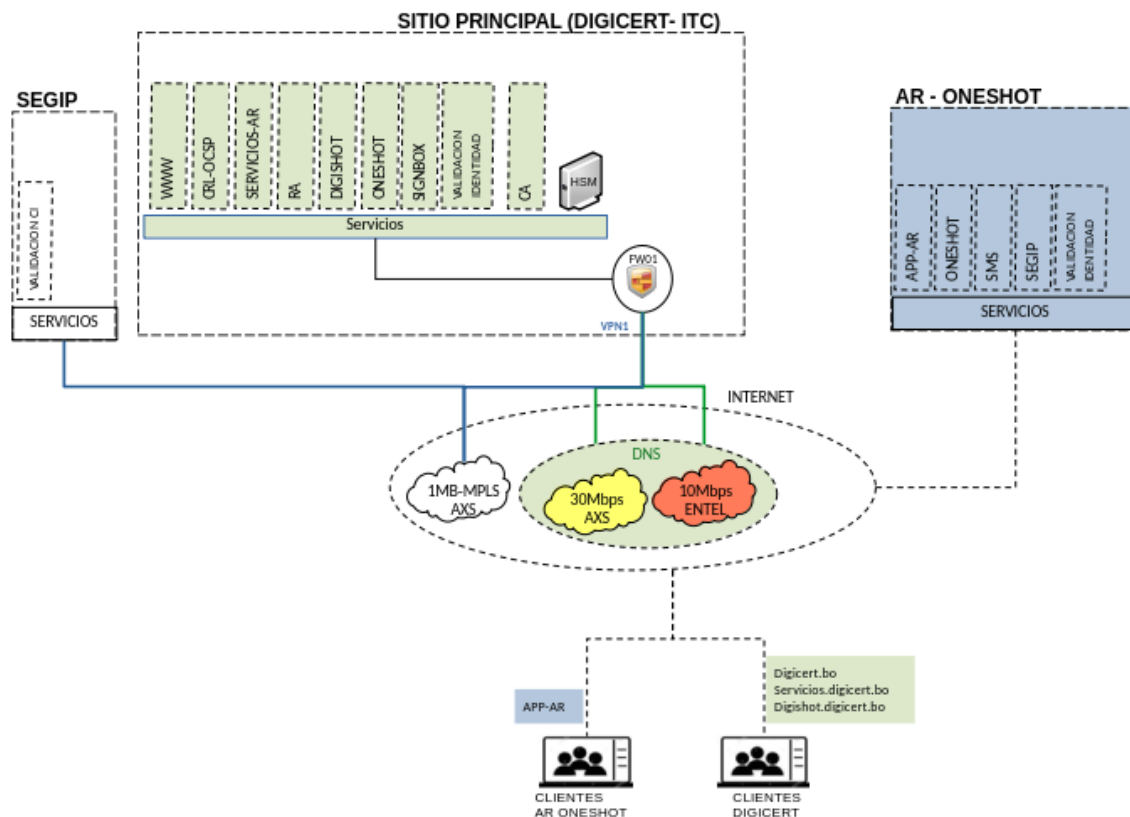
Término / Abreviatura	Definición
EJBCA	Herramienta para el firmado, emisión, revocación, suspensión y reactivación de certificados digitales.
NAT	Traducción de direcciones de Red (Network Address Translation)
AR	Agencia de Registro



PROCEDIMIENTO				
PROCEDIMIENTO CONEXIÓN DESDE AGENCIA DE REGISTRO HACIA LA ECA				
Código	PRO-ECA-29	Revisión	3	Página 3 de 4

7. DIAGRAMA DE INTERCONEXIÓN DE LA ECA DIGICERT Y ARS

El gráfico a continuación muestra cómo están interconectados los elementos de la red para que las AR puedan brindar el servicio necesario.



APP-AR, aplicación de la AR responsable de realizar la recolección de datos y validación de identidad del cliente que solicita el certificado digital. Esta aplicación es la que se comunica con ONESHOT.

ONESHOT, es el servidor por medio del cual se comunica la AR con la ECA DIGICERT para gestionar la emisión de certificados digitales de corta duración y de un solo uso (Perfil=DCNaturalCustodiaSimple). También gestiona la firma de los documentos que el usuario final solicita.

DIGISHOT, servidor por medio del cual se emiten certificados digitales de un solo uso y certificados de larga duración. Este servidor utiliza los servicios del servidor ONESHOT y SIGNBOX.

CA, tiene la siguiente configuración:

- Perfil, se tiene configurado un perfil con el nombre de DCNaturalCustodiaSimple, este perfil tiene los datos necesarios para la emisión del certificado.



PROCEDIMIENTO				
PROCEDIMIENTO CONEXIÓN DESDE AGENCIA DE REGISTRO HACIA LA ECA				
Código	PRO-ECA-29	Revisión	3	Página 4 de 4

SERVICIOS-AR, página web por medio de la cual un cliente final puede solicitar la emisión de certificados digitales pkcs11, pkcs12 software, custodia nube.

RA, página web por medio de la cual los operadores de digicert pueden gestionar la aprobación y emisión de los certificados digitales que los clientes digicert solicitan.

SERVICIOWEB-CA, interactúa con la CA para la emisión de certificados digitales, contiene los servicios web para que la web de servicios pueda gestionar los certificados.

PROVEEDOR SMS, realiza el envío de sms a los usuarios finales. Cuando un usuario:

- Solicita cambio de contraseña para ingresar a Servicios-AR.
- Realiza la firma de documentos utilizando ONESHOT.
- Realiza la solicitud de certificados digitales.

7.1. CONFIGURACIÓN ENTRE AR (ONESHOT) Y ECA DIGICERT

La AR-ONESHOT para brindar el servicio firma digital de un solo uso, debe contar con un servidor virtual ONESHOT, este servidor es entregado a la AR para que funcione dentro de su infraestructura.

El servidor virtual está configurado para interactuar con la ECA DIGICERT, para ello brinda servicios web, estos servicios son los que utiliza la AR-ONESHOT para integrar sus aplicaciones propietarias que interactúan con los clientes finales.

Para ver detalles de como instalar y configurar el servidor oneshot ver documento:

DIT-ECA-03 HABILITAR ONESHOT EN LA INFRAESTRUCTURA DE LA AR

8. ANEXOS

Anexo	Título / Nombre
N/A	

