RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

Integración de EREP con ECEP-RENIEC

Maria Paula Encinas Zevallos
Analista de Servicios PKI

GERENCIA DE CERTIFICACIÓN Y REGISTRO DIGITAL

SUB GERENCIA DE CERTIFICACIÓN E IDENTIDAD DIGITAL

MARZO 2018

Contenido

1. Software EJBCA
2. Perfiles Jerarquía Root 3 en el EJBCA
3. Web Service y Credenciales de acceso
4. Integración Class 2
5. Integración Class 3
6. Integración Class 4

Software de Gestión PKI (EJBCA)

- Software de Gestión de PKI basado en Java (JEE)
- Versión Community (libre) y versión Enterprise (licenciada)
- Realiza funciones de CA, RA y VA (CRL y OCSP)
- Múltiples jerarquías en una sola instancia de EJBCA

CA	• Autoridad que emite certificados • Autofirmada (Root) o subordinada
End Entity	• Usuario (persona, equipo, dominio) • No emiten certificados
Crytotoken	• Software • PKCS #11
Certificate Profile	• Key Usage • Extended Key Usage • OID Policy • CRL Distribution Point
End Entity Profile	• Subject DN del usuario • SAN del usuario

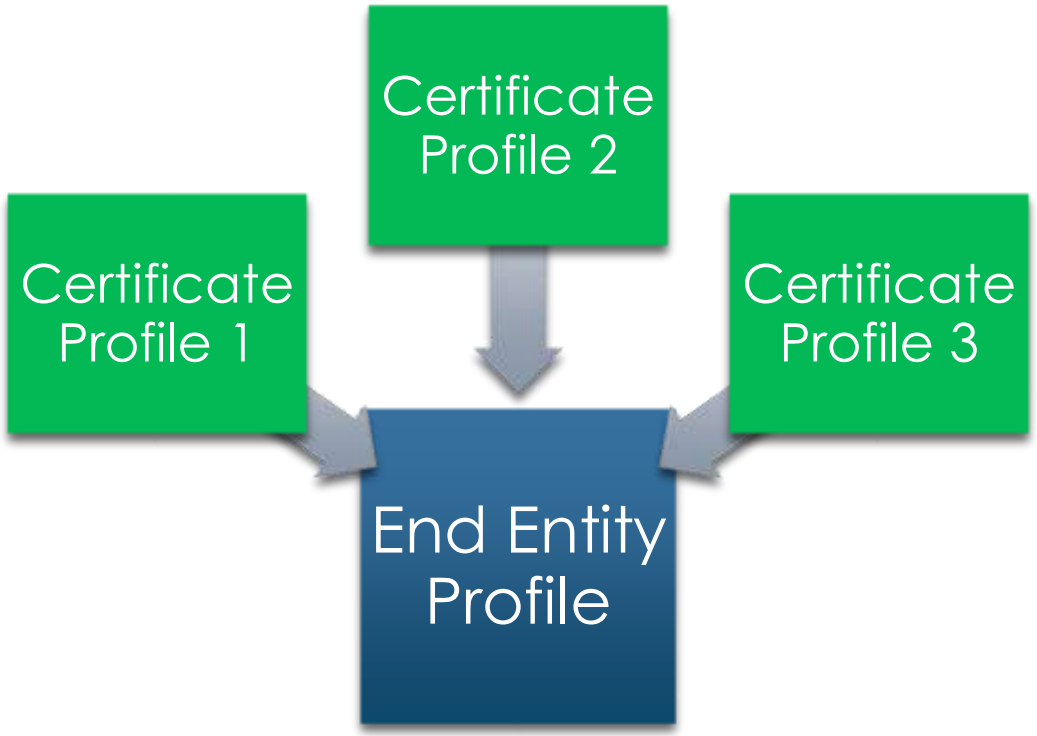
Crear un certificado de CA

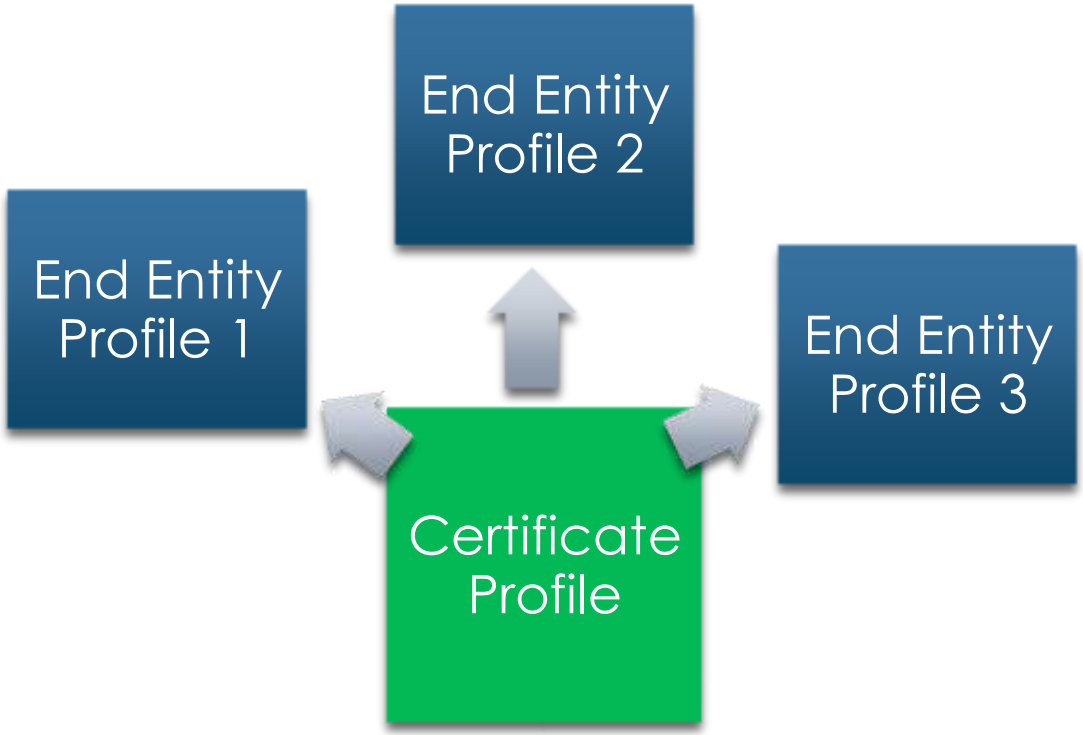
Certificado de End Entity (usuario)

- Subject DN del usuario
- SAN del usuario

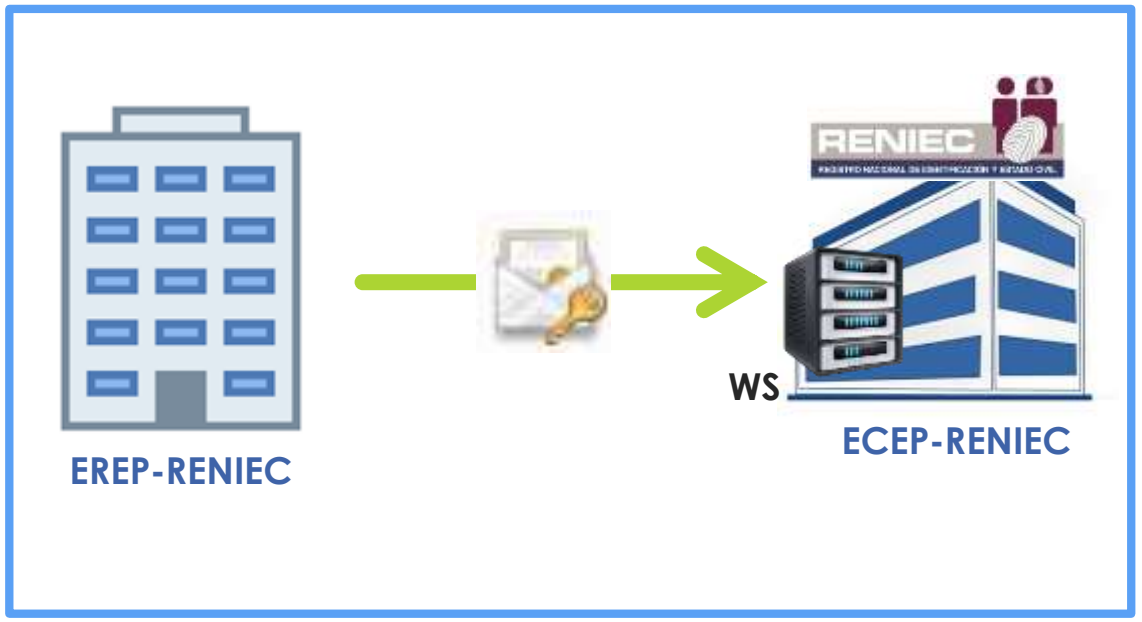
- Key Usage
- Extended Key Usage
- OID Policy
- CRL Distribution Point

Relación entre Certificate Profile y End Entity Profile





Web Service y credenciales de acceso



Administration

Manage Administrator Roles [?]

Roles

DCDelivery/Pepe	Administrators	Access Rules	Rename	Delete
DNIe	Administrators	Access Rules	Rename	Delete
EREP_RENIEC	Administrators	Access Rules	Rename	Delete
Genera CRL	Administrators	Access Rules	Rename	Delete
Mesa de Ayuda	Administrators	Access Rules	Rename	Delete
Super Administrator Role	Administrators	Access Rules	Rename	Delete

Add

Web Service

MÉTODO	RETORNO	ENTRADAS
findCerts	java.util.List<Certificate>	• String arg0 • boolean arg1
findUser	java.util.List<UserDataVOWS>	• UserMatch
certificateRequest	CertificateResponse	• UserDataVOWS • String • int • String • String
pkcs10Request	CertificateResponse	• String arg0 • String arg1 • String arg2 • String arg3 • String arg4
checkRevokationStatus	RevokeStatus	• String arg0 • String arg1
editUser	void	• UserDataVOWS var1
revokeCert	void	• String var1 • String var2 • int var3 • String var4

Este Web Service contiene 49 métodos; de los cuales, para acceder a los servicios brindados por la ECEP se requiere la utilización de siete (7) métodos

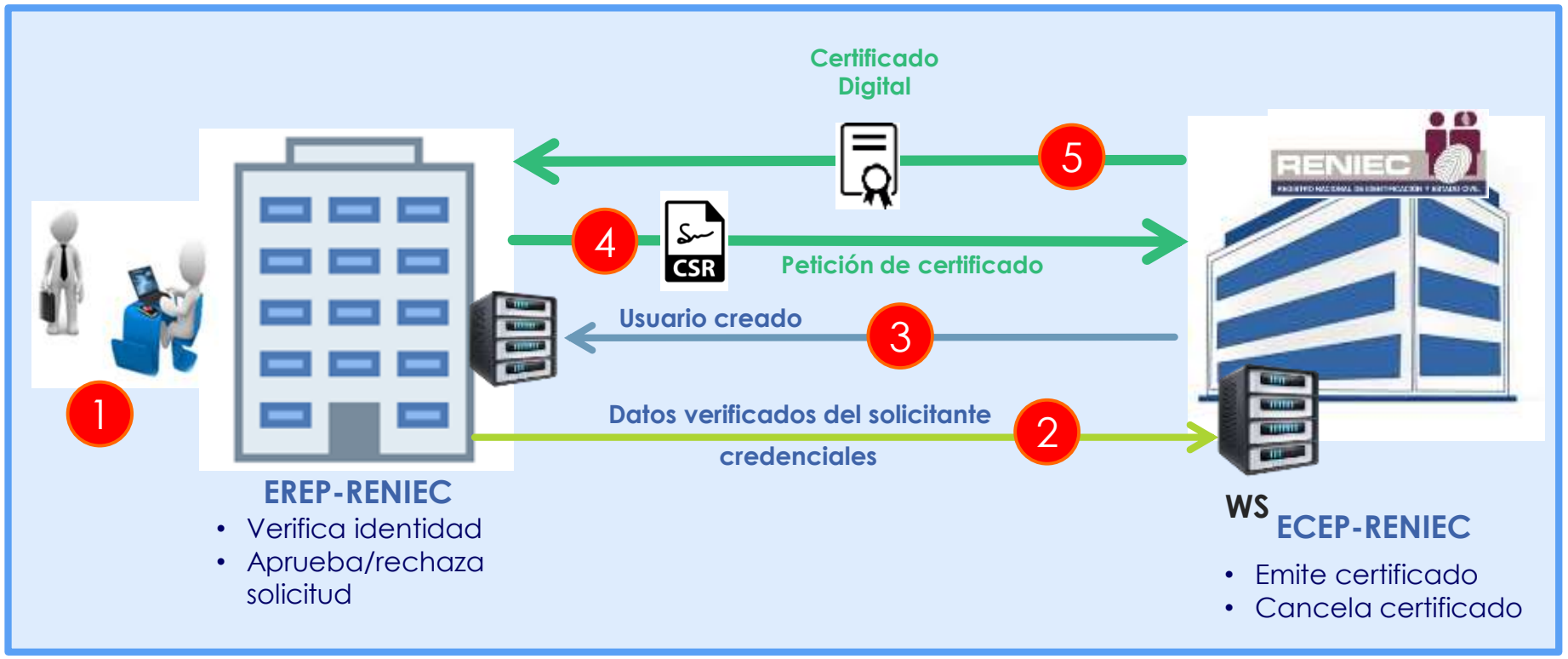
https://www.ejbca.org/docs/ws/index.html

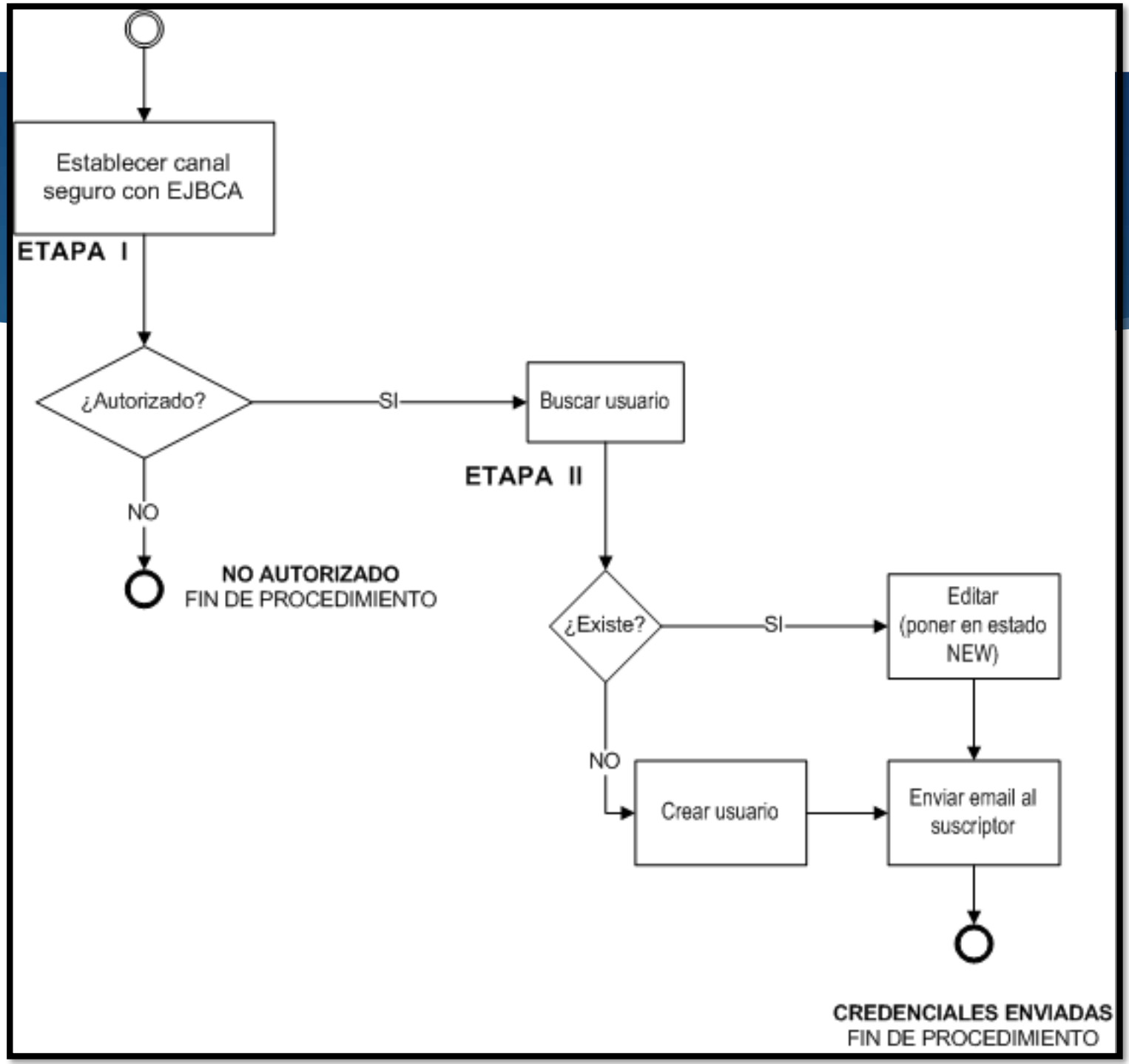
Anexo 03: Formato de username y parámetros del EJBCA

	Tipo	End Entity Profile	Username	Certificate Profile	CA
Class 1	FAU	<siglas>_Class1_EndEntityProfile	DNI:<número de DNI>FAU_<siglas>	Class 1_FAU_hard	ECEP30101
				Class 1_FAU_soft	
	P_FAU		DNI:<número de DNI>P_FAU_<siglas>	Class 1_P_FAU_hard	
				Class 1_P_FAU_soft	
Class 2	AUT	<siglas>_Class2_EndEntityProfile	DNI:<número de DNI>AUT_<siglas>	Class 2_AUT_hard	ECEP30201
	CIF		DNI:<número de DNI>CIF_<siglas>	Class 2_CIF_hard	
	FIR		DNI:<número de DNI>FIR_<siglas>	Class 2_FIR_hard	
	P_AUT		DNI:<número de DNI>P_AUT_<siglas>	Class 2_P_AUT_hard	
	P_CIF		DNI:<número de DNI>P_CIF_<siglas>	Class 2_P_CIF_hard	
	P_FIR		DNI:<número de DNI>P_FIR_<siglas>	Class 2_P_FIR_hard	
Class 3	CIF	<siglas>_Class3_EndEntityProfile	DNI:<número de DNI>CIF-RUC:<número de RUC>_<siglas>	Class 3_CIF_hard	ECEP30301
				Class 3_CIF_soft	
	FAU		DNI:<número de DNI>FAU-RUC:<número de RUC>_<siglas>	Class 3_FAU_hard	
				Class 3_FAU_soft	
	P_CIF		DNI:<número de DNI>P_CIF-RUC:<número de RUC>_<siglas>	Class 3_P_CIF_hard	
				Class 3_P_CIF_soft	
	P_FAU		DNI:<número de DNI>P_FAU-RUC:<número de RUC>_<siglas>	Class 3_P_FAU_hard	
				Class 3_P_FAU_soft	
Class 4	AA	<siglas>_Class4_AA_EndEntityProfile	RUC:<número de RUC>AA_<siglas>	Class 4_AA	ECEP30401
	P_AA		RUC:<número de RUC>P_AA_<siglas>	Class 4_P_AA	
	DC	<siglas>_Class4_DC_EndEntityProfile	RUC:<número de RUC>DC_<siglas>	Class 4_DC	
	P_DC		RUC:<número de RUC>P_DC_<siglas>	Class 4_P_DC	
	SSL	<siglas>_Class4_SSL_EndEntityProfile	RUC:<número de RUC>SSL_<siglas>	Class 4_SSL_TLS	
	P_SSL		RUC:<número de RUC>P_SSL_<siglas>	Class 4_P_SSL_TLS	

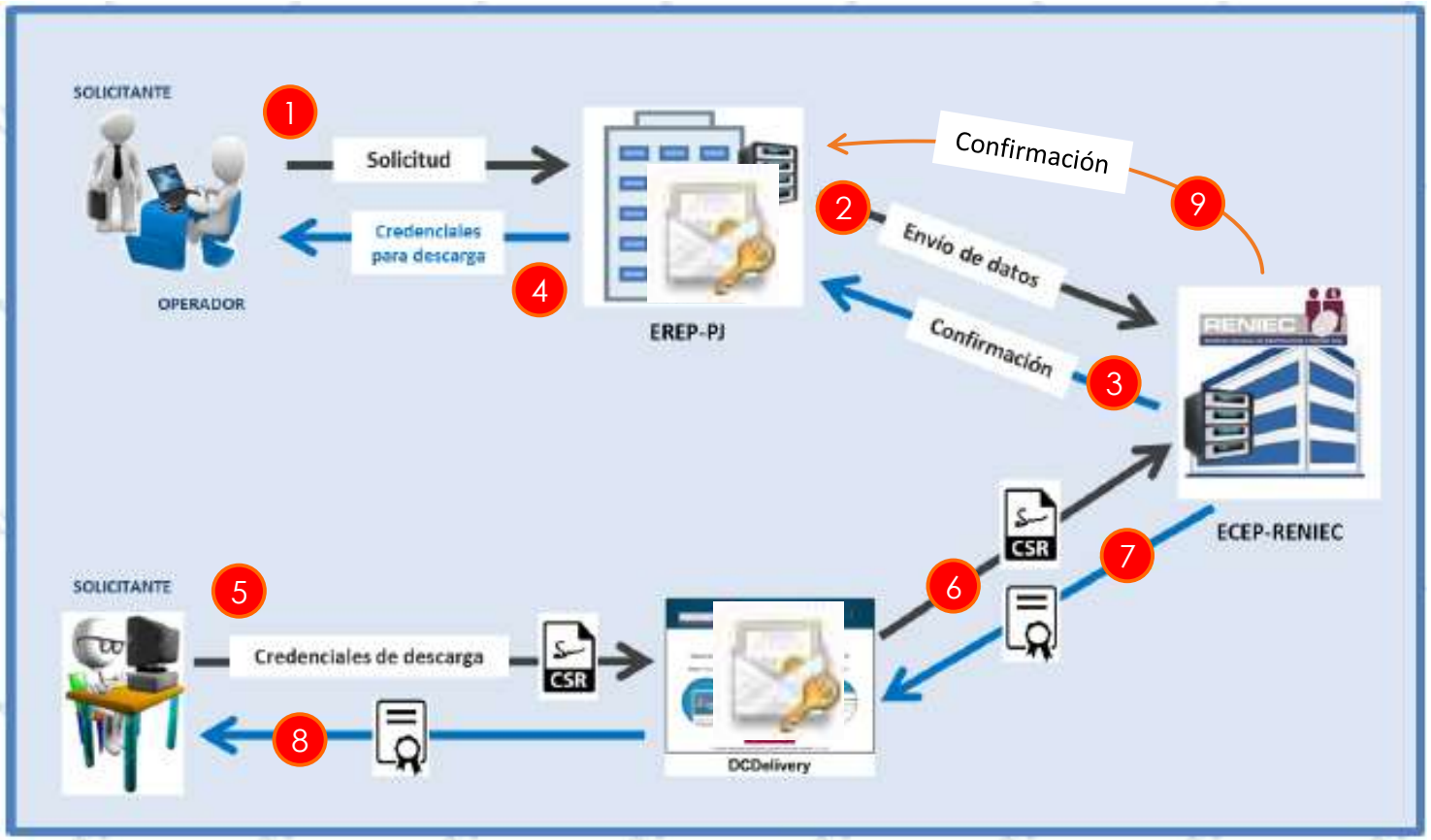
Nota: La ECEP-RENIEC definirá el valor de los campos donde aparece la variable <siglas>, por cada EREP.

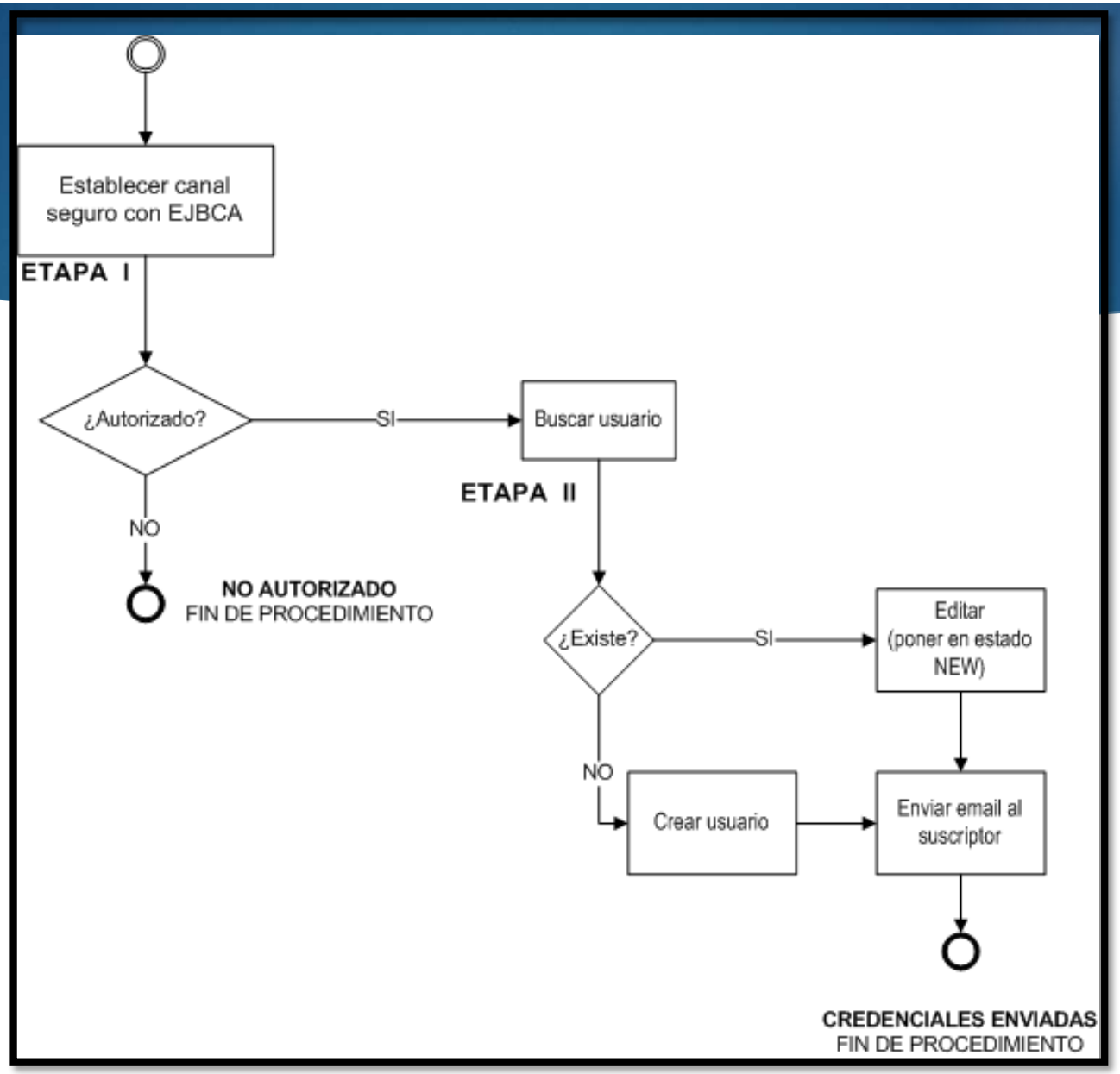
Integración ECEP y EREP (Class 2)



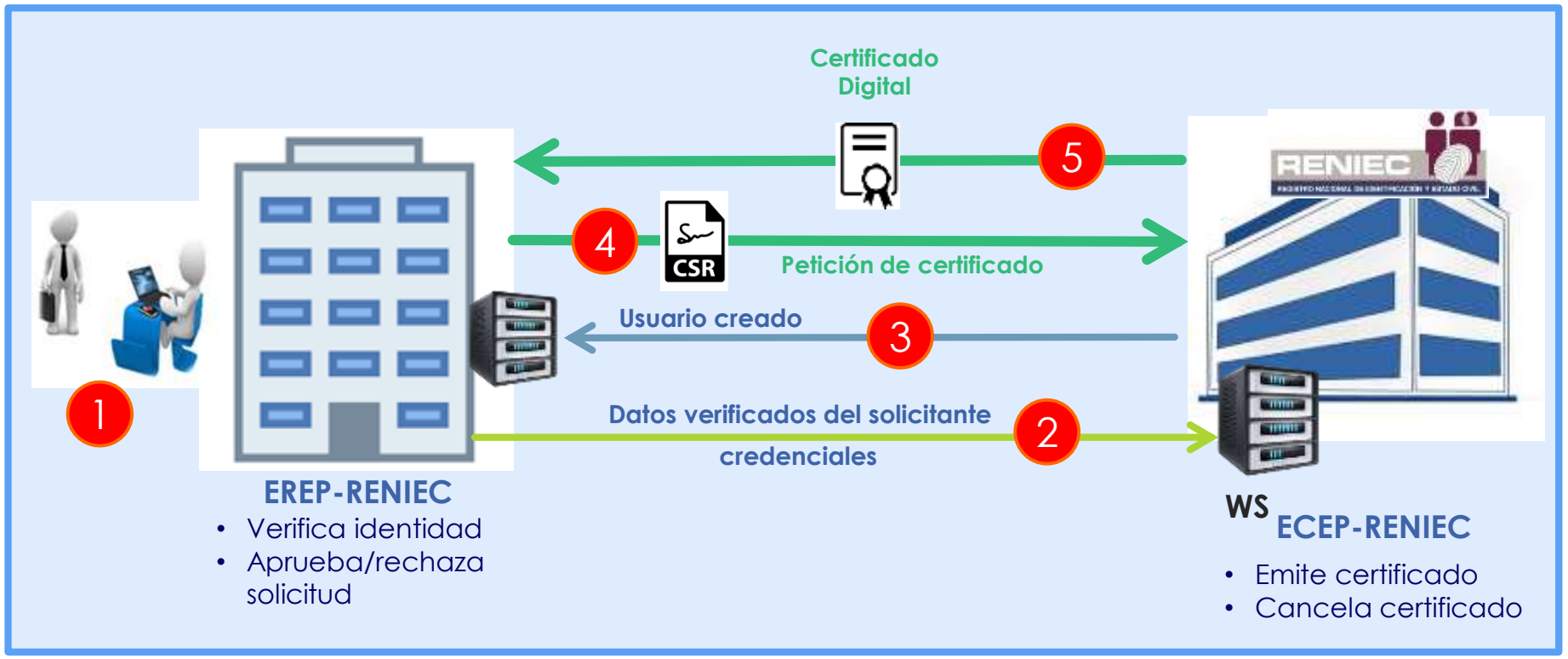

Establecer canal seguro con EJBCA
ETAPA I
¿Autorizado?
SI
Buscar usuario
ETAPA II
NO
NO AUTORIZADO
FIN DE PROCEDIMIENTO
¿Existe?
SI
Editar (poner en estado NEW)
NO
Crear usuario
Enviar email al suscriptor
CREDENCIALES ENVIADAS
FIN DE PROCEDIMIENTO

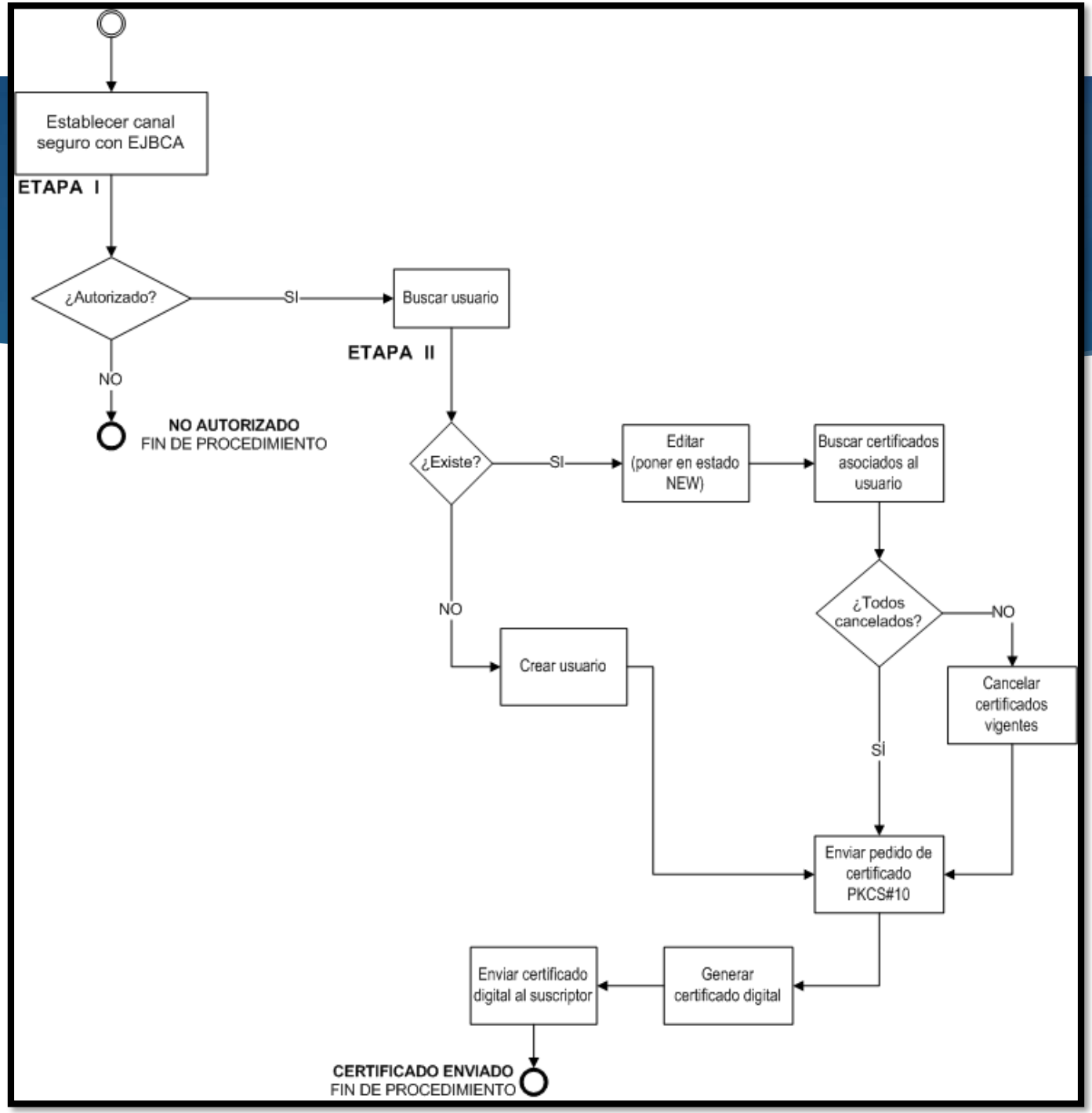
Integración ECEP y EREP (Class 3)




Establecer canal seguro con EJBCA
ETAPA I
¿Autorizado?
SI
Buscar usuario
ETAPA II
NO
NO AUTORIZADO
FIN DE PROCEDIMIENTO
¿Existe?
SI
Editar (poner en estado NEW)
NO
Crear usuario
Enviar email al suscriptor
CREDENCIALES ENVIADAS
FIN DE PROCEDIMIENTO

Integración ECEP y EREP (Class 4)




Establecer canal seguro con EJBCA
ETAPA I
¿Autorizado?
SI
Buscar usuario
ETAPA II
NO
NO AUTORIZADO
FIN DE PROCEDIMIENTO
¿Existe?
SI
Editar (poner en estado NEW)
Buscar certificados asociados al usuario
NO
Crear usuario
¿Todos cancelados?
NO
Cancelar certificados vigentes
SI
Enviar pedido de certificado PKCS#10
Enviar certificado digital al suscriptor
Generar certificado digital
CERTIFICADO ENVIADO
FIN DE PROCEDIMIENTO

AGENTE AUTOMATIZADO (AA)

- 2048 bits
- Algoritmo SHA256

Subject	CN	*<Nombre del Agente Automatizado>*	Sí
	O	*<Nombre de la Entidad>*	Sí
	OU	*<RUC de la entidad>*	Sí
	ST	*<Provincia-Departamento>*	Sí
	L	*<Distrito>*	Sí
	C	PE	Sí
	OI	*NTRPE-<número de RUC de la Entidad>*	No
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí

DOMAIN CONTROLLER (DC)

Subject	CN	*<Nombre del servidor Active Directory>*	Sí
	O	*<Nombre de la Entidad>*	Sí
	OU	*<RUC de la entidad>*	-
	ST	*<Provincia-Departamento>*	Sí
	L	*<Distrito>*	Sí
	C	PE	Sí
	OI	*NTRPE-<número de RUC de la Entidad>*	No
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí

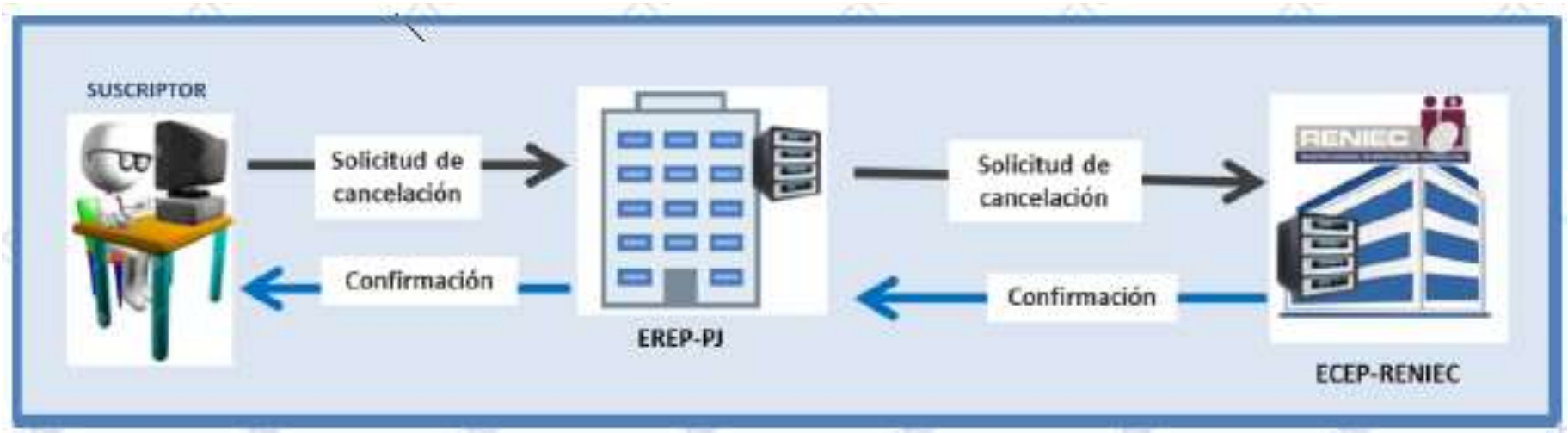
Subject Alternative Name	dNSName	*<Nombre DNS del Servidor Active Directory>*	Sí
	otherName	*<MS GUID = Globally Unique Identifier del Servidor Active Directory>*	Sí

CANAL CIFRADO(SSL/TLS)

Subject	CN	*<DNS, nombre FQDN o número de IP>*	Sí
	O	*<Nombre de la Entidad>*	Sí
	OU	*<RUC de la entidad>*	Sí
	ST	*<Provincia-Departamento>*	Sí
	L	*<Distrito>*	Sí
	C	PE	Sí
	SERIALNUMBER	-	No
	OI	*NTRPE-20295613620*	No
	OU	*EREP_PJ_<siglas de la EREP>_<código identificador de la transacción>*	Sí

Subject Alternative Name	dNSName	*<Nombre DNS del subdominio de *.reniec.gob.pe>*	Sí
	dNSName	*<Nombre DNS adicional del subdominio de *.reniec.gob.pe>*	No

Integración ECEP y EREP (Cancelación)



Perfiles por cada Clase

¡Gracias!