Microservicio MsCoreogCertificadosDigitales

Documento Versión: 1.0

Gestión de Seguridad Electrónica

Fecha generación: **02/12/2025**

CONTROL DE VERSIÓN

VERSIÓN	FECHA DE ACTUALIZACIÓN	CARGO	DESCRIPCIÓN
1.0	24/11/2025	Arquitecto de Software	Versión inicial del documento

Tabla de contenido

1 CONTEXTO

El Registro Nacional de Identificación y Estado Civil (RENIEC) es el organismo técnico autónomo encargado de la identificación de los peruanos, otorgar el Documento Nacional de Identidad (DNI) y registrar los hechos vitales. En el marco de la modernización y transformación digital del Estado peruano, RENIEC ha desarrollado el DNI Electrónico (DNIe), un documento de identidad que incorpora tecnología de chip y biometría, permitiendo la autenticación electrónica de ciudadanos y facilitando servicios digitales seguros.

2 INTRODUCCIÓN

Este documento describe el **catálogo de microservicios** identificados para la solución de Personalización del DNIe de RENIEC. El objetivo es establecer una arquitectura técnica moderna, escalable y mantenible que reemplace o complemente los sistemas monolíticos actuales mediante una transición ordenada hacia una arquitectura orientada a microservicios.

2.1 Justificación de la Arquitectura de Microservicios

La adopción de microservicios para esta solución responde a necesidades técnicas y operativas concretas:

Escalabilidad Independiente: Componentes con cargas diferenciadas pueden escalar de forma independiente según demanda real, optimizando recursos de infraestructura.

Resiliencia y Tolerancia a Fallos: El fallo de un microservicio no compromete servicios críticos. Los patrones Circuit Breaker y Retry garantizan continuidad operativa.

Agilidad en el Desarrollo: Equipos autónomos pueden desarrollar, probar y desplegar servicios de manera independiente, reduciendo tiempos de entrega.

Mantenibilidad y Evolución Tecnológica: Cada servicio puede evolucionar tecnológicamente sin afectar al ecosistema completo.

Trazabilidad y Observabilidad: Arquitectura distribuida permite implementar logging centralizado, distributed tracing y métricas granulares.

2.2 Arquitectura de Referencia

La solución se estructura en tres capas principales:

Capa de Exposición (API Management Layer): API Manager como punto único de entrada con gestión centralizada de seguridad, throttling y versionado.

Capa de Representación (Microservices Layer): Microservicios de negocio con lógica específica de dominio y responsabilidad única.

Capa de Integración (Integration Layer): Event Streaming para comunicación asíncrona y conectores a sistemas legados.

2.3 Códigos de Respuesta HTTP Estándar

Todos los microservicios implementan un conjunto estandarizado de códigos de respuesta HTTP para garantizar consistencia:

Código	Descripción
200	OK - Operación completada exitosamente
201	Created - Recurso creado exitosamente
400	Bad Request - Parámetros inválidos o datos incompletos
401	Unauthorized - Token JWT inválido, expirado o ausente
403	Forbidden - Sin permisos suficientes para ejecutar la operación

404	Not Found - Recurso no encontrado en el sistema
408	Request Timeout - Tiempo de espera agotado al conectar
409	Conflict - Conflicto con el estado actual del recurso
422	Unprocessable Entity - Datos válidos pero no procesables por reglas de negocio
429	Too Many Requests - Límite de rate limit excedido
500	Internal Server Error - Error interno del servicio (información generalizada al exterior, detalle en logs)
502	Bad Gateway - Servicio externo no disponible o respuesta inválida
503	Service Unavailable - Servicio temporalmente no disponible o Circuit Breaker abierto
504	Gateway Timeout - Servicio externo no respondió en tiempo esperado

3 CATÁLOGO DE MICROSERVICIOS

3.1 Microservicio MsCoreogCertificadosDigitales

El MsCoreogCertificadosDigitales es un microservicio de coreografía encargado de coordinar el flujo técnico de emisión del Certificado Digital DNIe.

Este microservicio actúa como un intermediario de negocio, aislando al SIIRC de la complejidad de la infraestructura PKI y ejecutando una secuencia garantizada de dos pasos obligatorios mediante el consumo directo de los siguientes endpoints del **MsAdaptadorPKI v1.0**:

- **Paso 1 – Generar Números de Solicitud PKI**

  POST /api/v1/adaptador/MsAdaptadorPKI/generarNumerosSolicitud2

- **Paso 2 – Emitir Certificado Digital DNIe**

  POST /api/v1/adaptador/MsAdaptadorPKI/generarCertificadoDigitalDniE

El coreógrafo administra los estados intermedios (`solicitudPkiId`), realiza las transformaciones de datos necesarias, registra los tiempos por paso, el manejo de fallas y entrega el certificado emitido.

3.1.1 Endpoint: Obtener Certificado Digital

Coordina el proceso completo de obtención de certificados digitales para un ciudadano, ejecutando secuencialmente la generación de par de claves y la emisión de certificados a través del sistema PKI.

Atributo	Valor
Path	/api/v1/coreog/MsCoreogCertificadosDigitales/obtener-certificado-digital
API Gateway	Interno
Método HTTP	POST
Protocolo	REST/HTTP
Headers	Authorization String(Bearer token JWT para autenticación) Content-Type String("application/json") X-Correlation-ID UUID(Identificador único de correlación para trazabilidad distribuida) X-Request-ID UUID(Identificador único de la solicitud) X-Office-Code String(Código de oficina donde se realiza la solicitud) X-Device-ID String(ID del dispositivo desde donde se origina la solicitud) X-Channel String(Canal de origen)

Entrada


```
{
  "solicitud": {
    "numeroDocumento": "string",
    "tipoDocumento": "string",
    "codigoSolicitudTramite": "string",
    "numeroTramite": "string"
  },
  "ciudadano": {
    "nombres": "string",
    "apellidoPaterno": "string",
    "apellidoMaterno": "string",
    "fechaNacimiento": "YYYY-MM-DDThh:mm:ssZ",
    "sexo": "string",
    "correoElectronico": "string",
    "departamento": "string",
    "provincia": "string",
    "distrito": "string"
  },
  "configuracionCertificados": {
    "tipoCertificados": ["string"],
    "vigenciaAnios": "integer",
    "usoExtendido": "boolean",
    "nivelSeguridad": "string"
  },
  "metadatos": {
    "oficinaOrigen": "string",
    "usuarioRegistrador": "string",
    "ipOrigen": "string",
    "timestampSolicitud": "YYYY-MM-DDThh:mm:ssZ"
  }
}
```


Respuesta


```
{
  "success": true,
  "data": {
    "transaccion": {
      "transaccionId": "string",
      "codigoSolicitudTramite": "string",
      "estado": "string",
      "fechaInicio": "YYYY-MM-DDThh:mm:ssZ",
      "fechaFin": "YYYY-MM-DDThh:mm:ssZ",
      "tiempoProcesamientoMs": "integer"
    },
    "ciudadano": {
      "numeroDocumento": "string",
      "nombreCompleto": "string"
    },
    "certificados": [
      {
        "tipoCertificado": "string",
        "certificadoId": "string",
        "numeroSerie": "string",
        "fechaEmision": "YYYY-MM-DDThh:mm:ssZ",
        "fechaVencimiento": "YYYY-MM-DDThh:mm:ssZ",
        "vigenciaAnios": "integer",
        "estadoCertificado": "string",
        "algoritmoFirma": "string",
        "longitudClave": "integer",
        "subjectDN": "string",
        "huellaCertificado": "string",
        "certificadoBase64": "string"
      }
    ],
    "pasosProceso": {
      "paso1GeneracionClaves": {
```

	"estado": "string",
	"solicitudPkiId": "string",
	"fechaInicio": "YYYY-MM-DDThh:mm:ssZ",
	"fechaFin": "YYYY-MM-DDThh:mm:ssZ",
	"intentos": "integer"
	},
	"paso2EmisionCertificado": {
	"estado": "string",
	"fechaInicio": "YYYY-MM-DDThh:mm:ssZ",
	"fechaFin": "YYYY-MM-DDThh:mm:ssZ",
	"intentos": "integer"
	}
	},
	"auditoria": {
	"registroAuditoriaId": "string",
	"usuarioEjecutor": "string",
	"oficinaEjecucion": "string",
	"ipCliente": "string"
	}
	},
	"metadata": {
	"timestamp": "YYYY-MM-DDThh:mm:ssZ",
	"correlationId": "string",
	"tiempoRespuesta": "string"
	}
	}

Error Response	"error": {
	"tipo": "string",
	"titulo": "string",
	"estado": 0,
	"errores": [
	{
	"detalleError": "string"
	}
	]
	}

3.1.1.1 Parámetros de Entrada

Dato	Atributo	Tipo	Obligatorio	Longitud Mínima	Longitud Máxima
Número de Documento	solicitud.numeroDocumento	String	Sí	8	12
Tipo de Documento	solicitud.tipoDocumento	String	Sí	2	3
Código Solicitud Trámite	solicitud.codigoSolicitudTramite	String	Sí	1	30
Número de Trámite	solicitud.numeroTramite	String	Sí	1	30
Nombres	ciudadano.nombres	String	Sí	1	100
Apellido Paterno	ciudadano.apellidoPaterno	String	Sí	1	50
Apellido Materno	ciudadano.apellidoMaterno	String	No	1	50

Fecha de Nacimiento	ciudadano.fechaNacimiento	String (ISO 8601)	Sí	10	10
Sexo	ciudadano.sexo	String	Sí	1	1
Correo Electrónico	ciudadano.correoElectronico	String	No	5	100
Departamento	ciudadano.departamento	String	Sí	1	50
Provincia	ciudadano.provincia	String	Sí	1	50
Distrito	ciudadano.distrito	String	Sí	1	50
Tipo de Certificados	configuracionCertificados.tipoCertificados	Array[String]	Sí	1	3
Vigencia en Años	configuracionCertificados.vigenciaAnios	Integer	Sí	1	4
Uso Extendido	configuracionCertificados.usoExtendido	Boolean	No	-	-
Nivel de Seguridad	configuracionCertificados.nivelSeguridad	String	No	4	10
Oficina de Origen	metadatos.oficinaOrigen	String	Sí	1	50
Usuario Registrador	metadatos.usuarioRegistrador	String	Sí	1	30
IP de Origen	metadatos.ipOrigen	String	No	7	45
Timestamp de Solicitud	metadatos.timestampSolicitud	String (ISO 8601)	Sí	20	30

3.1.1.2 Parámetros de Respuesta

Nombre	Tipo	Obligatorio	Descripción
success	Boolean	Sí	Indica si la operación fue exitosa.
data	Object	Sí	Contiene los datos principales de la transacción, ciudadano, certificados y auditoría.
data.transaccion	Object	Sí	Información asociada al proceso de transacción del trámite.
data.transaccion.transaccionId	String	Sí	Identificador único de la transacción.
data.transaccion.codigoSolicitudTramite	String	Sí	Código del trámite solicitado.
data.transaccion.estado	String	Sí	Estado actual de la transacción.
data.transaccion.fechaInicio	String (ISO 8601)	Sí	Fecha y hora en que inicia la transacción.

data.transaccion.fechaFin	String (ISO 8601)	No	Fecha y hora en que finaliza la transacción.
data.transaccion.tiempoProcesamientoMs	Integer	Sí	Duración total del proceso en milisegundos.
data.ciudadano	Object	Sí	Información del ciudadano asociado a la transacción.
data.ciudadano.numeroDocumento	String	Sí	Número de documento del ciudadano.
data.ciudadano.nombreCompleto	String	Sí	Nombre completo del ciudadano.
data.certificados	Array	Sí	Lista de certificados generados.
data.certificados[].tipoCertificado	String	Sí	Tipo de certificado emitido.
data.certificados[].certificadoId	String	Sí	Identificador único del certificado.
data.certificados[].numeroSerie	String	Sí	Número de serie del certificado.
data.certificados[].fechaEmision	String (ISO 8601)	Sí	Fecha y hora de emisión del certificado.
data.certificados[].fechaVencimiento	String (ISO 8601)	Sí	Fecha y hora de vencimiento del certificado.
data.certificados[].vigenciaAnios	Integer	Sí	Cantidad de años de vigencia del certificado.
data.certificados[].estadoCertificado	String	Sí	Estado actual del certificado.
data.certificados[].algoritmoFirma	String	Sí	Algoritmo criptográfico usado para firmar.
data.certificados[].longitudClave	Integer	Sí	Longitud de la clave usada en el certificado.
data.certificados[].subjectDN	String	Sí	Distinguished Name del sujeto del certificado.
data.certificados[].huellaCertificado	String	Sí	Huella digital del certificado.
data.certificados[].certificadoBase64	String	Sí	Certificado codificado en Base64.
data.pasosProceso	Object	Sí	Contenedor de las etapas del proceso del certificado.
data.pasosProceso.paso1GeneracionClaves	Object	Sí	Información del paso 1: generación de claves.
data.pasosProceso.paso1GeneracionClaves.estado	String	Sí	Estado del paso 1.
data.pasosProceso.paso1GeneracionClaves.solicitudPkiId	String	No	Identificador de la solicitud PKI.
data.pasosProceso.paso1GeneracionClaves.fechaInicio	String (ISO 8601)	Sí	Fecha de inicio del paso 1.

data.pasosProceso.paso1GeneracionClaves.fechaFin	String (ISO 8601)	No	Fecha de fin del paso 1.
data.pasosProceso.paso1GeneracionClaves.intentos	Integer	Sí	Número de intentos realizados.
data.pasosProceso.paso2EmisionCertificado	Object	Sí	Información del paso 2: emisión del certificado.
data.pasosProceso.paso2EmisionCertificado.estado	String	Sí	Estado del paso 2.
data.pasosProceso.paso2EmisionCertificado.fechaInicio	String (ISO 8601)	Sí	Fecha de inicio del paso 2.
data.pasosProceso.paso2EmisionCertificado.fechaFin	String (ISO 8601)	No	Fecha de fin del paso 2.
data.pasosProceso.paso2EmisionCertificado.intentos	Integer	Sí	Número de intentos realizados.
data.auditoria	Object	Sí	Datos de auditoría del proceso.
data.auditoria.registroAuditoriaId	String	Sí	Identificador del registro de auditoría.
data.auditoria.usuarioEjecutor	String	Sí	Usuario que ejecutó la transacción.
data.auditoria.oficinaEjecucion	String	Sí	Oficina desde donde se ejecutó la operación.
data.auditoria.ipCliente	String	Sí	Dirección IP del cliente que realizó la acción.
metadata	Object	Sí	Información complementaria de respuesta.
metadata.timestamp	String (ISO 8601)	Sí	Fecha y hora exacta de la respuesta.
metadata.correlationId	String	Sí	Identificador de correlación para trazabilidad.
metadata.tiempoRespuesta	String	Sí	Tiempo total de respuesta del servicio.
error	Object	No	Objeto que especifica algún error existente
error.tipo	String	No	Tipo de error
error.titulo	String	No	Título del error
error.estado	Integer	No	Código del estado de error
error.errores	Array	No	Listado de errores
error.errores[].detalleError	String	No	Detalle del error generado

3.1.1.3 Valores para el atributo statusCode

Código	Respuesta	Descripción
201	Created	Certificados emitidos exitosamente
400	Bad Request	Parámetros de entrada inválidos o incompletos
401	Unauthorized	Token JWT inválido, expirado o ausente
403	Forbidden	Usuario sin permisos para solicitar certificados
404	Not Found	Ciudadano no encontrado en el sistema
409	Conflict	Ya existe una solicitud de certificados en proceso para este ciudadano
422	Unprocessable Entity	Datos válidos, pero ciudadano no cumple requisitos para certificados
429	Too Many Requests	Límite de rate limit excedido
500	Internal Server Error	Error interno del microservicio
502	Bad Gateway	Error de comunicación con MsAdaptadorPKI
503	Service Unavailable	Servicio PKI temporalmente no disponible
504	Gateway Timeout	Timeout en comunicación con servicio PKI

Anexo1

TRANSFORMACIÓN DE DATOS

Esta sección documenta las transformaciones que el MsCoreogCertificadosDigitales realiza sobre los datos de entrada antes de invocar al MsAdaptadorPKI v1.0.

Transformación para Paso 1: generarNumerosSolicitud2

El coreógrafo transforma los datos de entrada para construir el request del endpoint generarNumerosSolicitud2.

Mapeo de Campos

Campo Destino (MsAdaptadorPKI)	Campo Origen (MsCoreog)	Regla de Transformación
tipoSolicitud	configuracionCertificados.tipoCertificados[0]	Primer tipo de certificado del array
cantidad	configuracionCertificados.tipoCertificados.length	Cantidad de tipos de certificado solicitados
prefijoPersonalizado	(opcional)	"CERT" como valor por defecto
metadatos.oficinaOrigen	metadatos.oficinaOrigen	Pasado directamente
metadatos.usuarioSolicitante	metadatos.usuarioRegistrador	**Renombrado**
metadatos.sistemaOrigen	(valor fijo)	"SIIRC"
metadatos.timestampSolicitud	metadatos.timestampSolicitud	Pasado directament

Transformación para Paso 2: generarCertificadoDigitalDniE

El coreógrafo transforma los datos de entrada para construir el request del endpoint generarCertificadoDigitalDniE, incluyendo el solicitudPkiId obtenido del Paso 1.

Mapeo de Campos

Campo Destino (MsAdaptadorPKI)	Campo Origen (MsCoreog)	Regla de Transformación
solicitudPkiId	(Paso 1 response)	**Valor obtenido del Paso 1**
numeroDocumento	solicitud.numeroDocumento	Pasado directamente
tipoDocumento	solicitud.tipoDocumento	Pasado directamente
ciudadano.nombres	ciudadano.nombres	Pasado directamente
ciudadano.apellidoPaterno	ciudadano.apellidoPaterno	Pasado directamente

ciudadano.apellidoMaterno	ciudadano.apellidoMaterno	Pasado directamente
ciudadano.nombreCompleto	(calculado)	Ver sección 4.2.2
ciudadano.fechaNacimiento	ciudadano.fechaNacimiento	Pasado directamente
ciudadano.sexo	ciudadano.sexo	Pasado directamente
ciudadano.correoElectronico	ciudadano.correoElectronico	Pasado directamente
configuracionCertificado.tipoCertificado	configuracionCertificados.tipoCertificados[i]	Iterar por cada tipo
configuracionCertificado.algoritmo	(valor fijo)	"RSA"
configuracionCertificado.longitudClave	(valor fijo)	2048
configuracionCertificado.vigenciaAnios	configuracionCertificados.vigenciaAnios	Pasado directamente
configuracionCertificado.usosClave	(derivado)	Ver sección 4.3.2
configuracionCertificado.usosExtendidos	(derivado)	Ver sección 4.3.2
datosSubject.commonName	(calculado)	= nombreCompleto
datosSubject.serialNumber	(calculado)	tipoDocumento + numeroDocumento
datosSubject.country	(valor fijo)	"PE"
datosSubject.organization	(valor fijo)	"RENIEC"
datosSubject.organizationalUnit	(valor fijo)	"ECEP"
metadatos.codigoSolicitudTramite	solicitud.codigoSolicitudTramite	Pasado directamente
metadatos.numeroTramite	solicitud.numeroTramite	Pasado directamente
metadatos.oficinaOrigen	metadatos.oficinaOrigen	Pasado directamente
metadatos.usuarioRegistrador	metadatos.usuarioRegistrador	Pasado directamente
metadatos.ipOrigen	metadatos.ipOrigen	Pasado directamente
metadatos.timestampSolicitud	metadatos.timestampSolicitud	Pasado directamente

Construcción de nombreCompleto

El MsAdaptadorPKI requiere el campo ciudadano.nombreCompleto que no está presente en la entrada del coreógrafo. Se calcula de la siguiente manera:

nombreCompleto = nombres + " " + apellidoPaterno + " " + apellidoMaterno

Reglas de construcción:

- Si apellidoMaterno está vacío o nulo, se omite del resultado
- Se eliminan espacios duplicados
- Se convierte a MAYÚSCULAS para compatibilidad con PKI
- Longitud máxima: 200 caracteres