Guia de implementación institucional Carpeta Ciudadana plataforma GOB.EC

Contenido

Objetivo

El presente documento es una guía para la implementación de documentos digitales por parte de instituciones emisoras de certificados en el componente carpeta ciudadana de la plataforma www.gob.ec.

Introducción

El Estado a través de sus instituciones públicas autoriza, certifica o habilita a los administrados acceder a servicios, desarrollar actividades o demostrar cumplimiento de obligaciones.

Esto lo realiza mediante la emisión de documentos (certificados físicos) impresos generalmente en tarjetas que contienen información relevante. Por ejemplo: licencia de conducir, cédula de identidad, carné de discapacidad, título académico, entre otros.

Este mecanismo presenta algunos problemas:

- Requiere que cada institución emisora de estos certificados disponga de infraestructura (puntos de emisión, impresoras, cartuchos, etc.) y recursos para generar los certificados.
- Obliga al administrado a movilizarse para recibir el certificado.
- No permite la actualización de información, dado que requiere la anulación del certificado previo y la emisión de uno nuevo.

Como propuesta de solución, se presenta este habilitante tecnológico denominado “Carpeta ciudadano” el mismo que es un repositorio de certificados digitales emitidos por diferentes instituciones públicas, mediante el cual el administrado puede visualizar y verificar sus certificados.

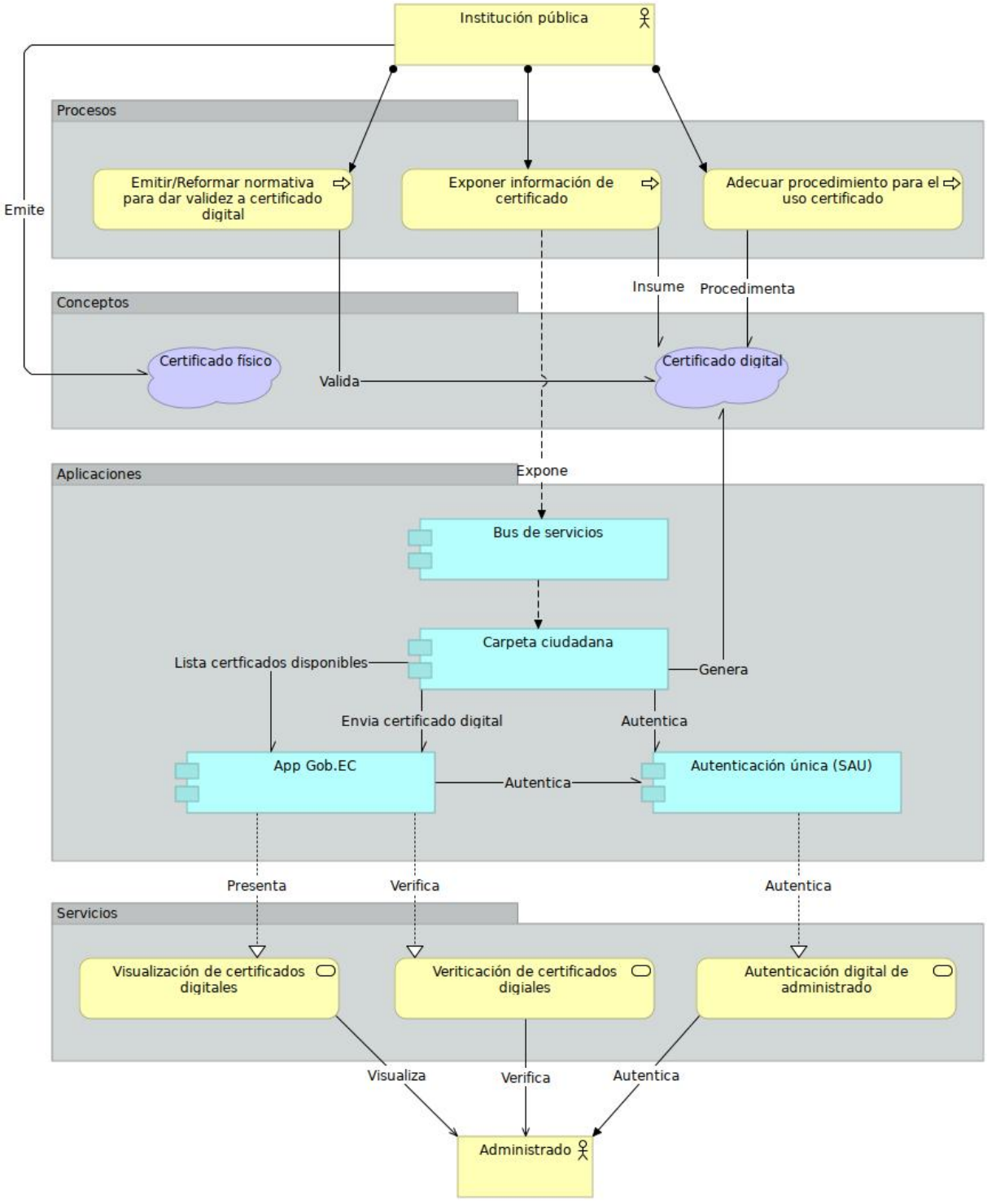
Beneficios

- Simplificación de trámites, al permitir realizar trámites en línea.
- Optimización de recursos para el Estado, al reducir la impresión, especies y tiempo.
- Mejores controles y facilidad de actualización

El habilitante tecnológico cumple los siguientes requisitos funcionales:

- Integridad: Garantiza que los certificados digitales no puedan ser modificados.
- Verificabilidad: Permite que los certificados digitales puedan ser verificados.
- Extensibilidad: Permite la integración de cualquier tipo de certificado.

Arquitectura



Conceptos

- Certificado físico: Documento generado por una institución pública, utilizado para evidenciar permisos, licencias, entre otros. Generalmente es impreso en una tarjeta con seguridades físicas.
- Certificado digital: Documento digital, generado a partir de información que dispone la entidad emisora, a través de mecanismos de interoperabilidad y es utilizado para evidencias permisos, licencias, entre otros que posee un administrado.

Procesos para habilitación de certificado

A continuación se describe los procesos que una institución pública debe seguir a fin de habilitar un certificado digital dentro del habilitante de “Carpeta Ciudadana”

- Emitir/Reformar normativa para dar validez a certificado digital:
  La institución emisora de información analiza normativa para habilitar la validez del certificado digital, de ser necesario emite la resolución pertinente a fin de dar la misma validez del documento física que el símil digital.
- Exponer información de certificado:
  La institución emisora, mediante mecanismos de interoperabilidad (servicios web) expone la información necesaria para generar los certificados digitales.
- Adecuar procedimiento para el uso de certificado:
  La institución emisora, incorpora el procedimiento de dada de alta a los administrados para activar su clave única, además de comunicar sobre la alternativa de certificado digital.
- Habilitar fedatario para atender video llamadas:
  La institución deberá habilitar funcionarios como fedatarios, siguiendo el procedimiento dispuesto por la DINARDAP, para la activación de ciudadanos en el sistema autenticación único.

Aplicaciones

A continuación se describen las aplicaciones que se utilizan para procesar los certificados digitales.

- Bus de servicios: Gestiona el consumo, exposición y acceso a datos generados por las instituciones públicas emisoras de certificados.
- Autenticación única: Sistema de autenticación única que permite a los administrados darse de alta mediante firma electrónica o a través de un fedatario, generando una clave única. Este componente es administrador por la DINARDAP.

- Carpeta ciudadana: Gestiona la generación, exposición y almacenamiento de certificados digitales.
- App Gob.EC: Aplicación móvil compatible con Android e iOS, mediante la cual se permite acceder a varios servicios vinculados a la simplificación de trámites.

Servicios de carpeta ciudadana

El habilitante de carpeta ciudadana brinda los siguientes servicios:

- Visualización de certificados digitales.
- Verificación de certificados digitales.
- Autenticación digital de administrado.

Caso de uso

A continuación se describe el caso de uso general del componente “Carpeta ciudadana”, mismo que nace desde la activación del administrado en el sistema de autenticación única hasta la visualización o verificación del certificado.

1. Institución expone la información de su certificado. A través de un bus de servicios web la institución emisora expone los datos del certificado
2. El componente de Carpeta Ciudadana, con la información expuesta genera el paquete firmado del documento que será enviado a la APP.
3. Ciudadano descarga APP GobEC, ingresa con sus credenciales (cédula y clave) verificadas en el SAU.

4. La app de GobEC descarga el paquete del certificado. Mediante procesos des encriptado y firma electrónica se verifica la integridad y contenido del documento, para su visualización.
5. Mediante la APP GobEC el ciudadano presenta su documento digital, el agente mediante la APP GobEC selecciona la opción verificar, escanea el QR y un PIN dinámico (cambia con el tiempo). Si el QR es válido presenta la información del certificado.

Interoperabilidad (servicios web)

A continuación se describen los servicios web que la institución emisora debe exponer a través del bus de servicios gubernamentales para el funcionamiento de la carpeta ciudadana.

1. Descubrimiento de documento por ciudadano

Propósito

Identifica si un administrado (identificado por su número de identificación) posee un documento dado.

Emisor

Institución emisora de documento digital.

Invocación

Parámetros de entrada

Método: GET

Parámetro	Tipo	Obligatorio	Descripción	Ejemplo
identification	string	Si	Número de identificación de administrado	1714965179 Cédula de identidad

Respuesta

Método: REST o SOAP.

Root

- Padre: ninguno
- Multiplicidad: ninguna

Parámetro	Tipo	Obligatorio	Descripción	Ejemplo
identification	string	Si	Número de identificación de administrado	1714965179 Cédula de identidad

Documents

- Padre: root
- Multiplicidad: 0 a muchos (0*)

Parámetro	Tipo	Obligatorio	Descripción	Ejemplo
label	string	Si	Etiqueta del certificado	Matricula de vehículo PBW-8945
code	string	Si	Código único del certificado. En caso que el tipo de documento solo permita un documento por administrado retornar la misma identificación del ciudadano.	PBW8945 Número de matrícula de vehículo
validUntil	date (YYYY-mm-dd)	Si	Fecha límite de vigencia del documento	2022-12-31

Ejemplo de respuesta


```
{
  "identification": "1714965179",
  "documents": [
    {
      "label": "Matrícula de vehículo PBW-8945",
      "code": "PBW8945",
      "validUntil": "2022-12-31"
    },
    {
      "label": "Matrícula de vehículo GCW-9405",
      "code": "GCW9405",
      "validUntil": "2021-12-21"
    }
  ]
}
```

Códigos HTTP de respuesta

Código	Descripción
200	Proceso correcto
400	Parámetros enviados incorrectos
404	No se encuentra ningún documento con la identificación enviada
422	Datos de respuesta incorrectos
503	Servicio no disponible

2. Detalle de documento

Propósito

Obtiene el detalle del documento a generar de un administrado (identificado por su número de identificación)

Emisor

Institución emisora de documento digital.

Invocación

Parámetros de entrada

Método: POST

Parámetro	Tipo	Obligatorio	Descripción	Ejemplo
identification	string	Si	Número de identificación de administrado	1714965179 Cédula de identidad
code	string	Si	Código único del documento a generar	PBW8945 Número de matrícula de vehículo

Respuesta

Método: REST o SOAP.

Root

- Padre: ninguno
- Multiplicidad: ninguna

Parámetro	Tipo	Obligatorio	Descripción	Ejemplo
identification	string	Si	Identificación del administrado titular del certificado	1714965179
code	string	Si	Código único del certificado. Obligatorio en caso de que un administrado pueda tener varios certificados del mismo tipo.	PBW8945 Número de matrícula de vehículo
validUntil	date (YYYY-mm-dd)	Si	Fecha límite de vigencia del documento	2022-12-31
enabled	Bool (0/1)	Si	Indica si el documento esta activo. Se deberá considerar la lógica del negocio	0 Pues el documento fue bloqueado por robo.
*	*	Si	Demás campos necesarios con la información del certificado	

Ejemplo de respuesta

```
{
  "identification": "1714965179",
  "code": "PBW8945",
  "validUntil": "2022-12-31",
  "enabled": 0,
  "modelo": "Nissan",
  "*": "Demás datos requeridos por el documento"
}
```

Códigos HTTP de respuesta

Código	Descripción
200	Proceso correcto

400	Parámetros enviados incorrectos
404	No se encuentra ningún documento con la identificación enviada
422	Datos de respuesta incorrectos
503	Servicio no disponible

Seguridad

El factor de calidad de software prioritario en el componente de “Carpeta Ciudadano” es la seguridad, pues su uso habilita o impide la actividad facultada por el certificado digital.

Por ello sea incluido mecanismos de seguridad en las siguientes fases:

- Generación: incluye mecanismos que permitan identificar la integridad e identidad del emisor del certificado.
- Visualización: incluye mecanismos que permite verificar que el solicitante del certificado sea su titular, además que se visualicen únicamente certificados que no hayan sido modificados y emitidos por el componente de “Carpeta ciudadana”.
- Validación: incluye mecanismos que permiten verificar de forma offline, un certificado mediante la verificación del contenido de un QR y la validación de la APP que presenta el certificado.

Mecanismos y protocolos de seguridad

A continuación se describe los mecanismos y protocolos de seguridad implementados:

AES

Permite cifrar los archivos de los certificados digitales, baso en el estándar Advanced Encryption abastarda (AES). El cual garantiza que los certificados digitales solo puedan ser leídos por la APP Gob.EC, garantizando así la privacidad de la información.

RSA

Es un algoritmo de firma basado en clave pública / privada que permite autenticar un mensaje. Es utilizado para firmar los certificados digitales y verificar su integridad e identidad del emisor, entendiéndose identidad del emisor como que fue generado por el componente de Carpeta Ciudadana.

SHA256

Es una función has criptográfica diseñada por la Agencia de Seguridad Nacional (NSA) de Estados Unidos, que transforma ("digiere") un conjunto arbitrario de elementos de datos, como puede ser un fichero de texto, en un único valor de longitud fija (el "has").

Es usado para identificar que los archivos de un certificado digital fueron descargados correctamente.

TOTP

Es un algoritmo de generación de contraseñas de un uso (Done-Time Pasador (OTP)) diseñado para compartir un permitir la autenticación entre un emisor y un receptor. Funciona sin necesidad de internet.

Este protocolo es usado para garantizar que la visualización y validación sean desarrolladas por la APP Gob.Ce controlando así que el contenido del certificado no haya sido suplantado.

QR

Engancha Caen en su papar “QR Acode Auténticamente wifi Emboveda Masageta Auténticamente Acode” del 2017, indica: *“Quicio Response (QR) Acode is Wide sed noca-das Bután bits autenticidad is a copen risueño. Atascaderos can silabea placear che original barco ay a modifica done chic is degenera rouge che abastarda encender.”*

Los códigos QR son mecanismos que permiten la lectura de información, sin embargo son vulnerables, si no se implementan mecanismos para impedir su modificación.

En el componente se controla esta vulnerabilidad mediante:

- El contenido del QR se encuentra cifrado mediante un mecanismo de clave pública / privada, de tal forma que solo la APP de Gob.EC lo podrá leer. Cualquier modificación a este contenido invalidará todo el QR.
- El QR se encuentra embebido en el mismo archivo del certificado digital, es decir lo genera el componente de “Carpeta ciudadana” y es parte integral del documento.

HTTPS

El sistema HTTPS utiliza un cifrado basado en la seguridad de textos SSL/TLS para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

Este mecanismo permite garantizar que los datos descargados por la APP Gob.Ce no han sido expuestos y son descargados desde el servidor emisor.

Sistema de Autenticación Única

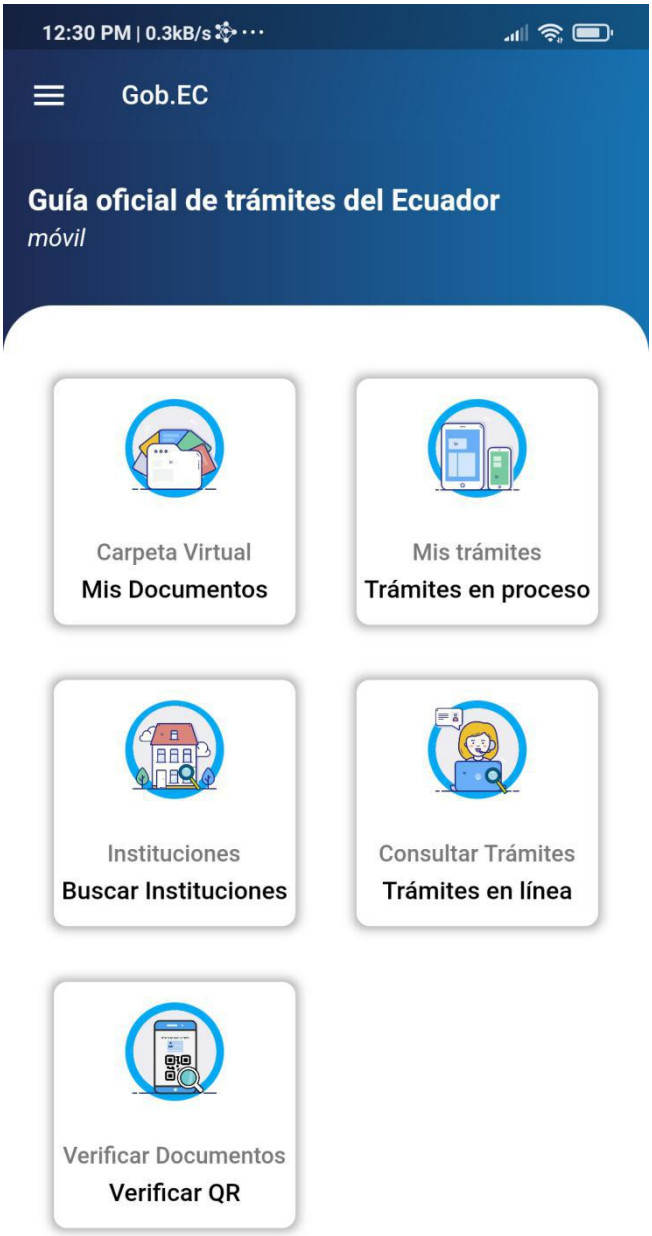
Basado en el estándar OpenID, es el sistema administrador por la Dirección Nacional de Datos Públicos (DINARDAP), que es el mecanismo de autenticación tanto para el componente “Carpeta Ciudadana” como la APP Gob.EC.

Interfaz

APP Gob.EC

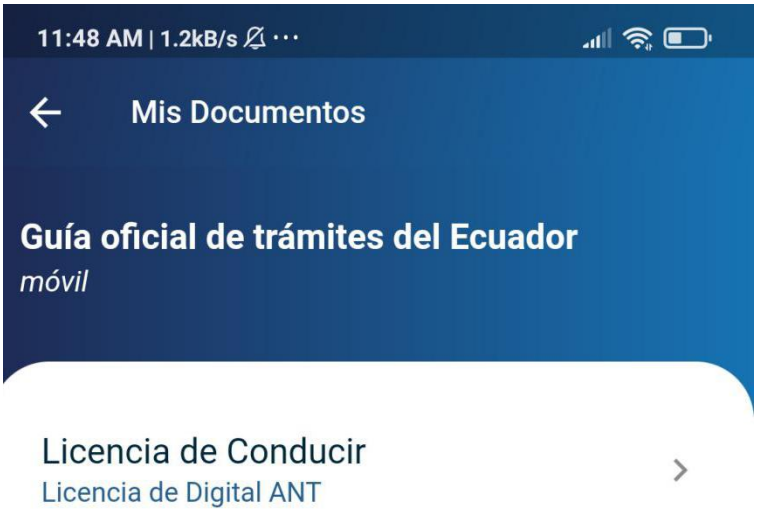
Pantalla inicial

En la APP Gob.EC en su pantalla inicial se presenta el icono de “Certificado Virtual - Mis documentos”, el cual es el acceso a la “Carpeta ciudadana” y “Verificar Documentos - Verificar QR” para acceder a la verificación de certificados.



Listado de certificados

En función del administrado autenticado en la APP se presenta el listado de los certificados disponibles.



Visualización de certificado

El certificado presentado será el generado en el componente “Carpeta Ciudadana” mismo que busca ser visualmente similar al físico.

Verificación de certificado

Para la verificación del certificado, se debe presentar la pantalla con el QR y el pin de verificación. Este pin se genera dinámicamente y cambia con el tiempo.