Plataforma de Administración Electrónica

Consejería de Fomento y Medio Ambiente

D.G. de Telecomunicaciones

Introducción a Cl@ve

Junta de Castilla y León

Octubre 2016

Área de Desarrollo y Mantenimiento

Junta de Castilla y León

Cl@ve:

Sistema para la identificación electrónica del ciudadano ante las Administraciones Públicas.

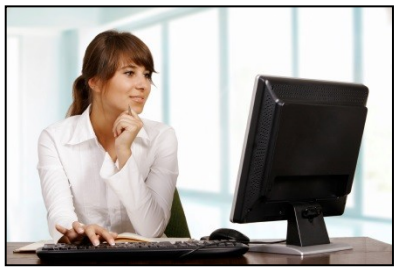
Admite la posibilidad de ser utilizado como sistema de identificación ante el sistema de Firma en la nube *Cl@ve-nb*.

Es un servico de cobertura nacional, de libre adhesión por parte de las AA.PP. que admite identificación mediante certificado y claves concertadas para aquellos ciudadanos que se inscriban en el servicio

- **Cl@ve ocasional** (Cl@ve PIN): sistema de contraseña de validez muy limitada en el tiempo, orientado a usuarios que acceden esporádicamente a los servicios, que se corresponde con el sistema PIN24H de la AEAT.
- **Cl@ve permanente** : sistema de contraseña de validez duradera en el tiempo, pero no ilimitada, orientado a usuarios habituales. Se corresponde con el sistema de acceso mediante usuario y contraseña, reforzado con claves de un solo uso por SMS, a los servicios de Seguridad Social. Este sistema será además el que permitirá el acceso al ciudadano a la firma en la nube .

Cl@ve:

Esquema de funcionamiento



Cl@ve:

Requisitos de funcionamiento

Cl@ve independiza la provisión del servicio de la gestión de credenciales de acceso.

El proveedor del servicio simplemente indica el nivel de confidencialidad de los datos que va a proveer, y Cl@ve devuelve al ciudadano los sistemas de autenticación cuya confiabilidad es acorde al nivel de confidencialidad

Requisitos para el ciudadano:

- Darse de alta en el sistema Cl@ve
- Opcionalmente:
  - Disponer de un teléfono móvil
  - Disponer de un certificado electrónico

Requisitos para la Administración:

- Adscribirse al sistema
- Hacerse cargo de las contrapartidas económicas derivadas del envío de SMS al ciudadano
- Integrar el servicio con el sistema Cl@ve
- Establecer el nivel de confidencialidad del servicio que quiera ofrecerse a través de Cl@ve

Junta de Castilla y León

Cl@ve:

Confidencialidad vs. confiabilidad

Existen diferentes mecanismos de autenticación, cuyo grado de confiabilidad varía dependiendo de factores técnicos y organizacionales.

Factores organizacionales: afectan a la fase de registro del usuario:

- ¿Qué calidad tiene el proceso de identificación?
- ¿Qué calidad tiene la forma de entrega de la credencial?
- ¿Qué calidad tiene la entidad que entrega la credencial?

Factores técnicos, afectan a la fase autenticación vía electronica, e incluyen*:*

- El tipo y robustez de la credencial (por ejemplo, un token)
- Las características de seguridad con que cuenta el mecanismo de autenticación remota

El mayor o menor grado de confiabilidad de un mecanismo de autenticación implicará la materialización de determinados riesgos.

A partir del estudio de la relación entre mecanismos de autenticación y riesgos materializables, el proyecto STORK de la Unión Europea ha definido los *niveles de Garantía de la Calidad en la Autenticación para procesos electrónicos* en el ámbito de los países miembro, o niveles QAA – *Quality of Authentication Assurance*

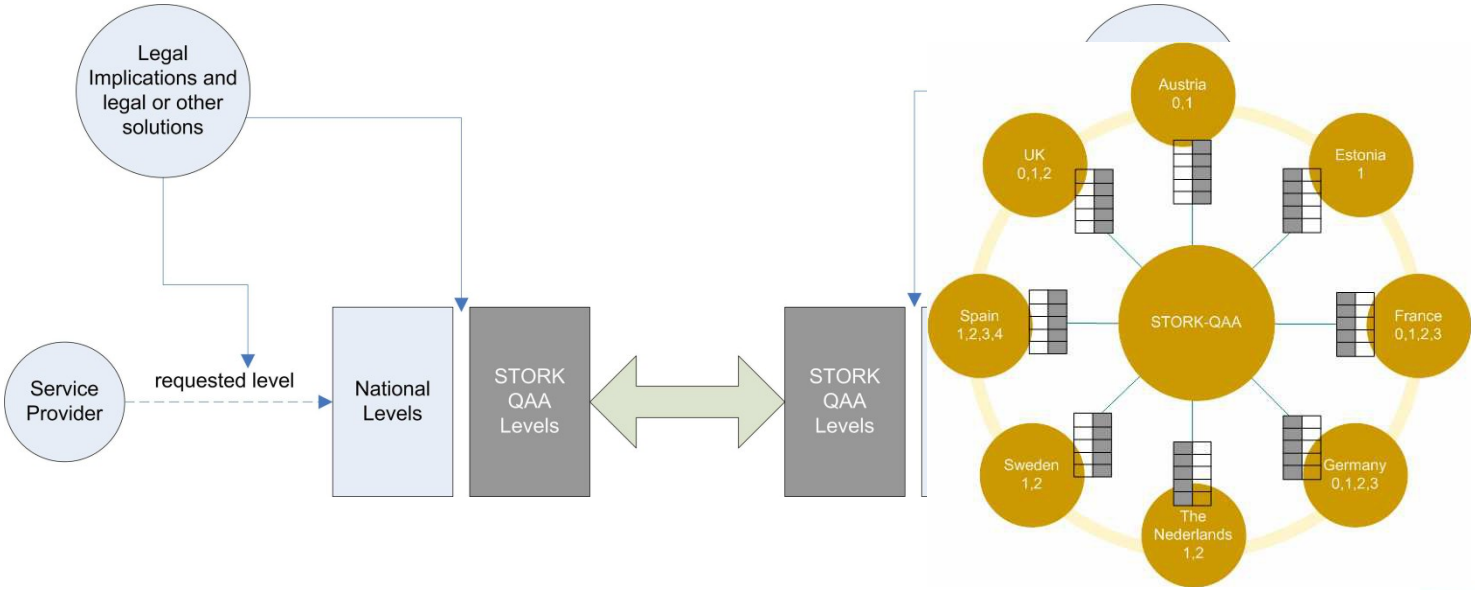
Junta de Castilla y León

Cl@ve:

Niveles QAA

Los niveles QAA son comunes en toda la UE, pero cada estado les asimila a su propia legislación

Nivel STORK QAA	Descripción
1	Sin garantía, o garantía mínima
2	Garantía baja
3	Garantía sustancial
4	Garantía alta



Cl@ve:

LOPD y niveles QAA

La legislación española en esta materia queda regulada en la LOPD, cuya asimilación a los niveles QAA se muestra a continuación.

	STORK-QAA tentative Level 1	STORK-QAA tentative Level 2	STORK-QAA tentative Level 3	STORK-QAA tentative Level 4
Austria				Level 1
Belgium	Level 1	Level 2	Level 3	Level 4
Estonia		Level 1 (with username and passwords and rotating passwords)	Level 1(one-time password token)	Level 1(with ID-card or Mobile ID)
France			Level 1	Level 2, Level 3
Germany	Level 0	Level 1	Level 2	Level 3
Iceland	Level 1	Level 2	Level 3	Level 4
Italy		Level 1 (PIN + password)		Level 1 (digital certificate in smart card)
Luxemburg				Level 1, Level 2
The Netherlands		Level 1	Level 2	
Portugal		Level 1		Level 3
Slovenia	Level 1		Level 2	Level 3
Spain	Level 1	Level 1	Level 2	Level 3
Sweden				Level 1, Level 2
UK	Level 0	Level 1	Level 2	

Table 16: Resume of the preliminary mapping, for each member states, between the national levels and the STORK-QAA tentative levels.

Cl@ve:

Servicios al ciudadano y niveles LOPD

Los servicios ofrecidos a través de Administración Electrónica son básicamente de dos tipos:

Remisión de información: generalmente implica el respaldo de esa información, es decir, explicitar quién se responsabiliza la veracidad de la información, o acreditar quién expresa voluntad o da consentimiento:

- Ciudadano: solicitudes, anexos, documentación complementaria
- Administración: notificación de documentos de resolución, o de demanda de información

El mecanismo a emplear es la firma electrónica

Recuperación de información: implica mostrar en pantalla datos o documentos electrónicos. Las medidas de acceso a esta información deben ser conformes a la confidencialidad de la información mostrada.

El mecanismo a emplear es la autenticación previa del usuario

Junta de Castilla y León

Cl@ve:

Asignación de niveles LOPD a la información para el ciudad

Es el Órgano Gestor responsable del Procedimiento Administrativo quien conoce qué información va a ponerse a disposición del ciudadano, y qué nivel LOPD debería asociarse.

El documento CCN-STIC-803, "*Guía de seguridad - Esquema Nacional de Seguridad, Valoración de los sistemas*" puede constituir una referencia para valorar la información y asignarla al nivel LOPD correcto.

La correcta interpretación de dicho nivel LOPD, respecto de la confidencialidad de los datos, es responsabilidad exclusiva del Órgano Gestor.

Los técnicos de Informática son los responsables de que el servicio desarrollado invoque al sistema Cl@ve con el nivel QAA establecido por el Órgano Gestor a partir del nivel LOPD.

Junta de Castilla y León

Cl@ve:

Relación entre niveles en Cl@ve y credenciales requeridas

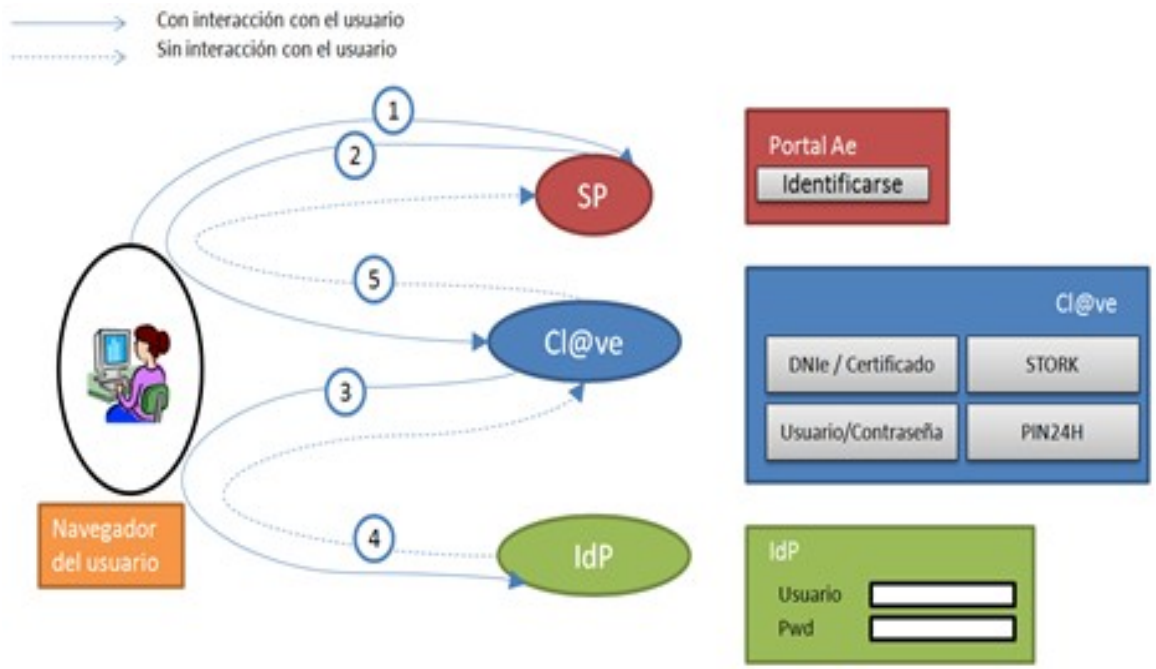
Nivel en Cl@ve	Nivel de Registro	Modo de registro	Credencial
2 (bajo)	Básico	Telemático a partir de datos conocidos, basado en CSV	Clave PIN Clave Permanente sin OTP
	Fuerte	Presencial, telemático con certificado electrónico reconocido o sistemas equivalentes.	Clave Permanente sin OTP
3 (medio)	Fuerte	Presencial, telemático con certificado electrónico reconocido o sistemas equivalentes.	Clave PIN Clave Permanente reforzada con OTP (SMS al móvil) Certificado reconocido en soporte SW
4 (alto)	Fuerte	Presencial, telemático con certificado electrónico reconocido o sistemas equivalentes.	DNI electrónico Otros certificados reconocidos en soporte HW, con la certificación de una entidad de certificación acreditada.

Cl@ve:

Descripción de la solución

Aislamiento entre el Proveedor del Servicio, el Proveedor de Identidad y el Sistema Cl@ve

El nexo de unión es la página web del ciudadano: mecanismo basado en redirecciones



***SP**: Service Provider*
***IdP**: Identity Provider*

2.- Servicio que invoca (SP), nivel de calidad de iID exigido, firmado por SP

3.- Servicio que invoca (SP), nivel de calidad de iID exigido, firmado por Cl@ve

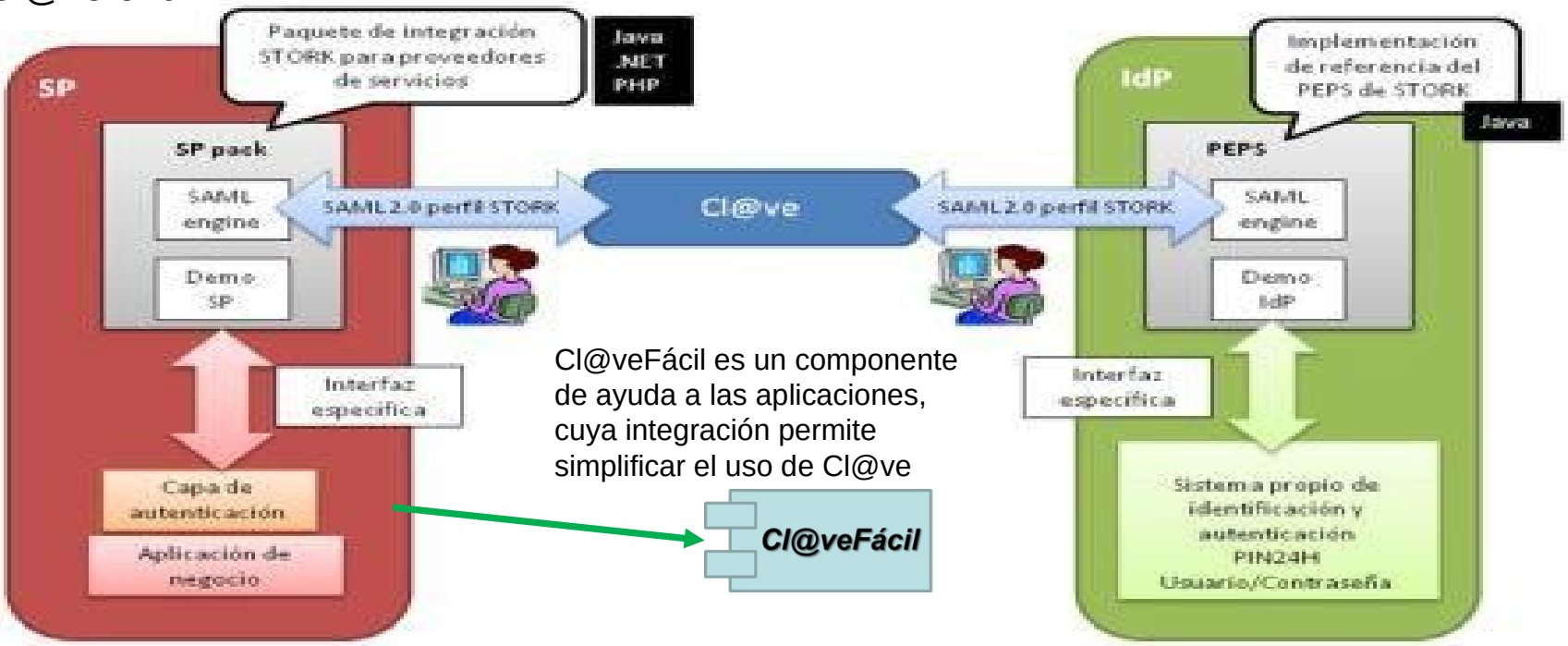
4.- Respuesta de la identificación, firmada por IdP

5.- Respuesta de la identificación, firmada por Cl@ve

Cl@ve:

Arquitectura de la solución

Desde el servidor de la JCyL, la aplicación en él alojada genera páginas HTML en el navegador del ciudadano, en cuyo código se implementan las redirecciones necesarias a Cl@ve e IdP



***Nota**: La información de identidad viaja en formato XML, en concreto en SAML v2.0, con mapeos de los elementos del XML a las necesidades de identificación del proyecto Stork*

Cl@ve:

Tareas para la integración

- *Identificar el servicio y asignarle el nivel LOPD*

  El servicio se entiende como el aplicativo que devuelve un conjunto de datos (*activo de información*), bien como información en una página web, o bien como un documento electrónico. El nivel LOPD se aplica sobre ese conjunto de datos, y debe ser asignado por el funcional, o bien asignado por un técnico informático, pero aprobado por el técnico funcional. El mayor nivel de seguridad requerido entre todos los activos de información determinará el nivel de identificación de Cl@ve.

- *Asignar el nivel QAA a partir del nivel LOPD*

  Técnico informático: ver primera columna de la tabla en la transparencia 9

- *Modificar el interfaz de la aplicación para integrar* Cl@veFácil

  Técnico informático: requiere adaptaciones en el código HTML, y un par de invocaciones a sendos *servlets*

- *Pruebas de integración y funcionales*

  Técnico informático: se realizarían pruebas desde el entorno de PRE de la aplicación contra el sistema Cl@ve en Preproducción

Junta de Castilla y León

Cl@ve:

Ejemplo de petición

```
DatosSolicitudClave datosSolicitudClave = new DatosSolicitudClave();

datosSolicitudClave.setUrlClave(urlClave);
datosSolicitudClave.setUrlRetorno(urlRetorno);
datosSolicitudClave.setSectorProveedor(sectorProveedor);
datosSolicitudClave.setNombreProveedor(nombreProveedor);
datosSolicitudClave.setAplicacionProveedor(aplicacionProveedor);
datosSolicitudClave.setQaa(Qaa.POCA_SEGURIDAD);
datosSolicitudClave.setRutaFirma(RUTA_CONFIG + NOMBRE_RUTA_FIRMA);

// ******** Tipo de autenticación requerida, por defecto son todas **********
datosSolicitudClave.definirListaIdp(Idp.AFIRMA, Idp.STORK, Idp.AEAT, Idp.SEGSOCIAL);

// *************** Preparar objeto petición **********************
ClaveFacil claveFacil = ClaveFacil.getInstance();

response.setContentType("text/html");
ServletOutputStream outServlet = response.getOutputStream();
try {
   PeticionClave peticion = claveFacil.prepararSolicitudClave(datosSolicitudClave);
   claveFacil.realizarSolicitudClave(peticion, outServlet);
   outServlet.flush();
   outServlet.close();
} catch (ClaveExcepcion e) {
   log.error("doGet - Error durante la generación de la petición a Cl@ve", e);
   outServlet.println("ERROR: " + e.getMessage());
} catch (Throwable e) {
   log.error("doGet Throwable - Error durante la generación de la petición a Cl@ve", e);
   outServlet.println("ERROR: " + e.getMessage());
} finally {
   outServlet.close();
}
```

Junta de Castilla y León

Cl@ve:

Ejemplo de tratamiento de respuesta

```
String SAMLResponse = request.getParameter(ClaveFacil.PARAMETRO_SAML_RESPUESTA);
String remoteHost = (String) request.getRemoteHost();
response.setContentType("text/html");
ServletOutputStream outServlet = response.getOutputStream();
try {
   // Se decodifica la respuesta
   ClaveFacil claveFacil = ClaveFacil.getInstance();
   DatosRespuestaClave respuestaClave = claveFacil.procesarRespuestaClave(SAMLResponse, remoteHost);

   log.debug("Respuesta decodificada correctamente");

   // Valores devueltos por Cl@ve. Atributos básicos
   boolean respuestaClaveError = respuestaClave.isError();
   String mensajeClave = respuestaClave.getMensaje();
   String emisor = respuestaClave.getEmisor();
   String idUsuario = respuestaClave.recuperarValorAtributoAdicional(AtributosBasicos.IDENTIFICADOR.getValor());

   // Listado con los atributos recuperados
   for (String atributo : respuestaClave.recuperarNombreAtributosAdicionales()) {
      System.out.println(atributo + ": " + respuestaClave.recuperarValorAtributoAdicional(atributo));
   }
   System.out.println("NIF : " + IdentificadorClave.obtenerCodigoCiudadano(idUsuario));
   System.out.println("Pais 1: " + IdentificadorClave.obtenerCodigoPais1(idUsuario));

} catch (ClaveExcepcion e) {
   log.error("ERROR: durante la respuesta de Cl@ve", e);
} finally {
   outServlet.flush();
   outServlet.close();
}
```

Junta de Castilla y León

Muchas gracias