



La tarjeta electrónica de identificación
sanitaria en Extremadura
y su aplicación en un proyecto piloto de
receta electrónica
(Aspectos técnicos)

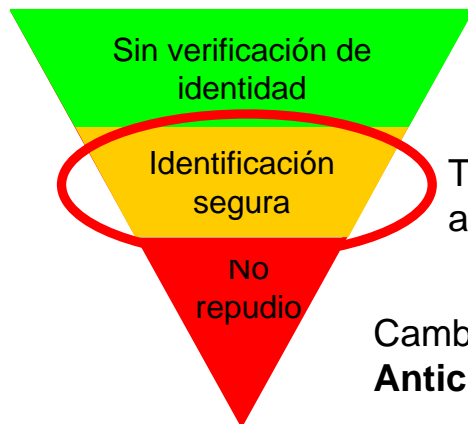
Club de usuarios Civitas 2008



Posicionamiento del proyecto

- El cumplimiento de la ley 11/2007 y la modernización de los sistemas de información en la asistencia sanitaria, con proyectos como la historia clínica electrónica y la receta electrónica demandan **medios de identificación electrónica seguros**, tanto del asegurado como del profesional
- Disponer de medios de identificación segura es la base para la **prestación de servicios por vía electrónica**
- No obstante, diferentes tipos de acceso requieren **diferentes niveles de identificación**, lo que apunta a la posibilidad de un despliegue progresivo de las soluciones

e-Servicios para el asegurado



Ej. Servicios prestados actualmente por vía telefónica. **Cita Previa**,...

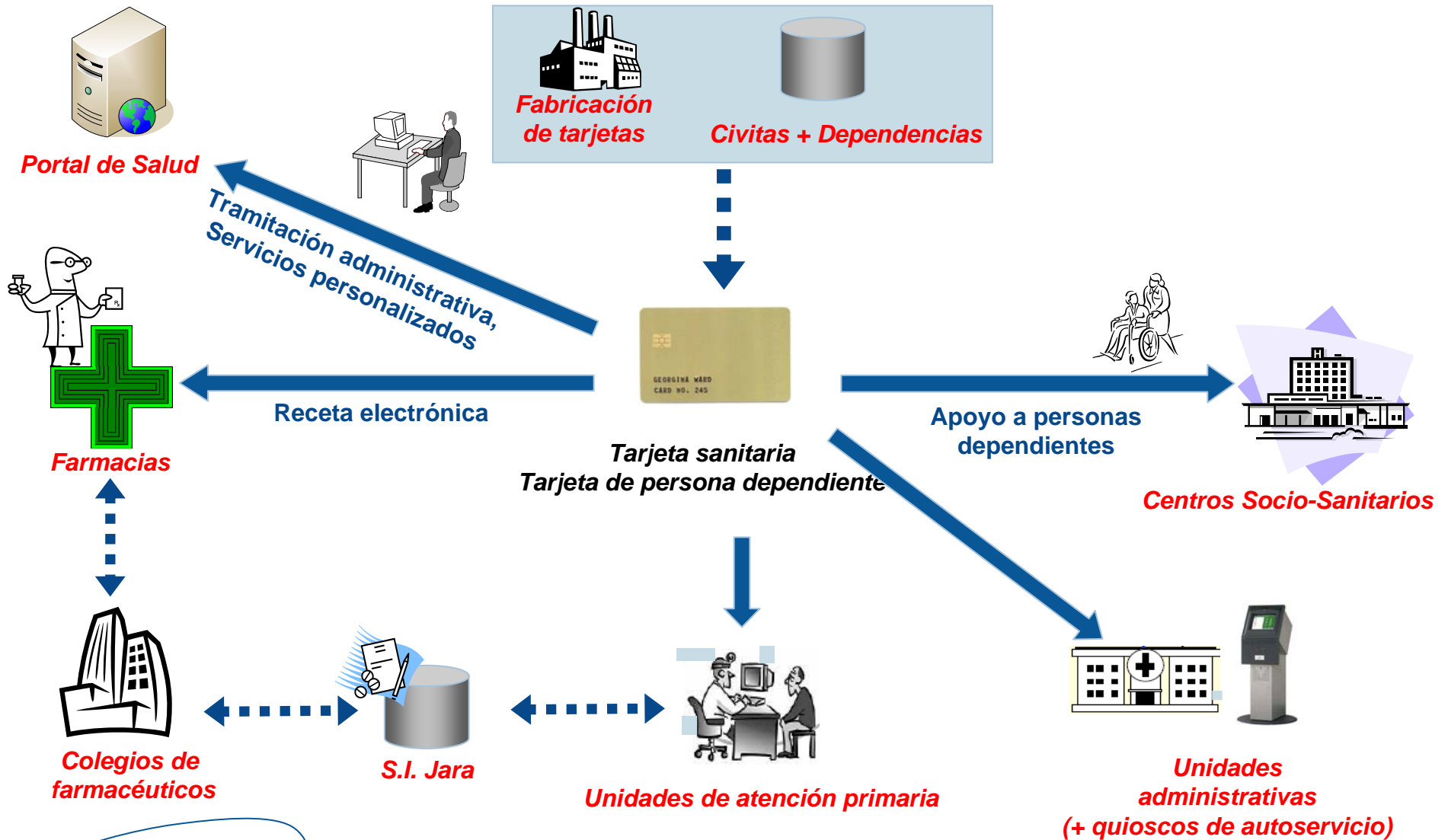
Trámites administrativos (algunos), acceso al dato clínico asistencial, **Receta Electrónica**

Cambio de médico, solicitud de ayudas, registro de **Voluntades Anticipadas**,...

El proyecto de la Consejería de Sanidad y Dependencia de la Junta de Extremadura tiene por objetivo proporcionar un medio de identificación seguro para los asegurados el cual permita el acceso a información protegida y la eliminación del fraude



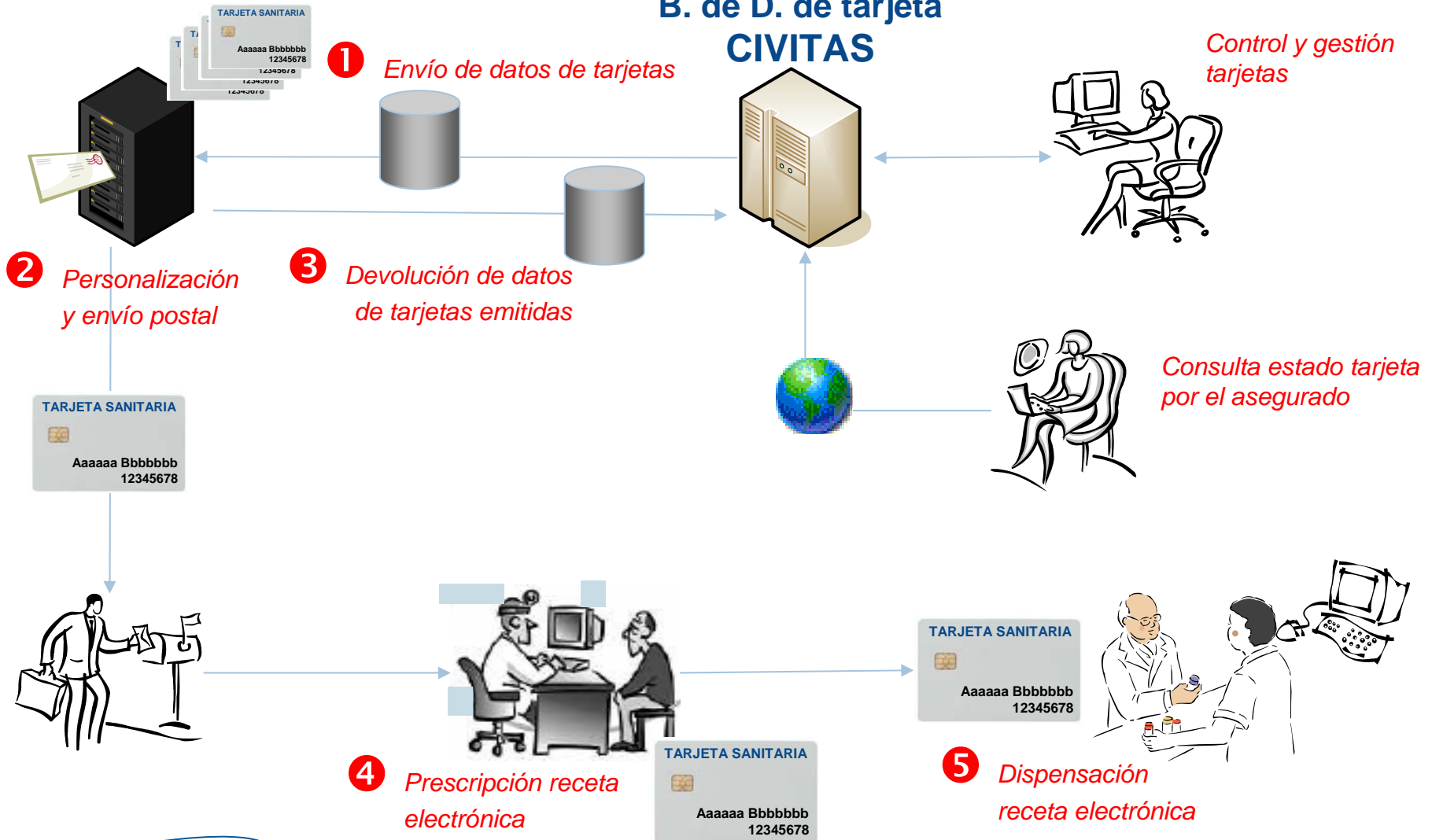
Usos y agentes: la visión a medio plazo



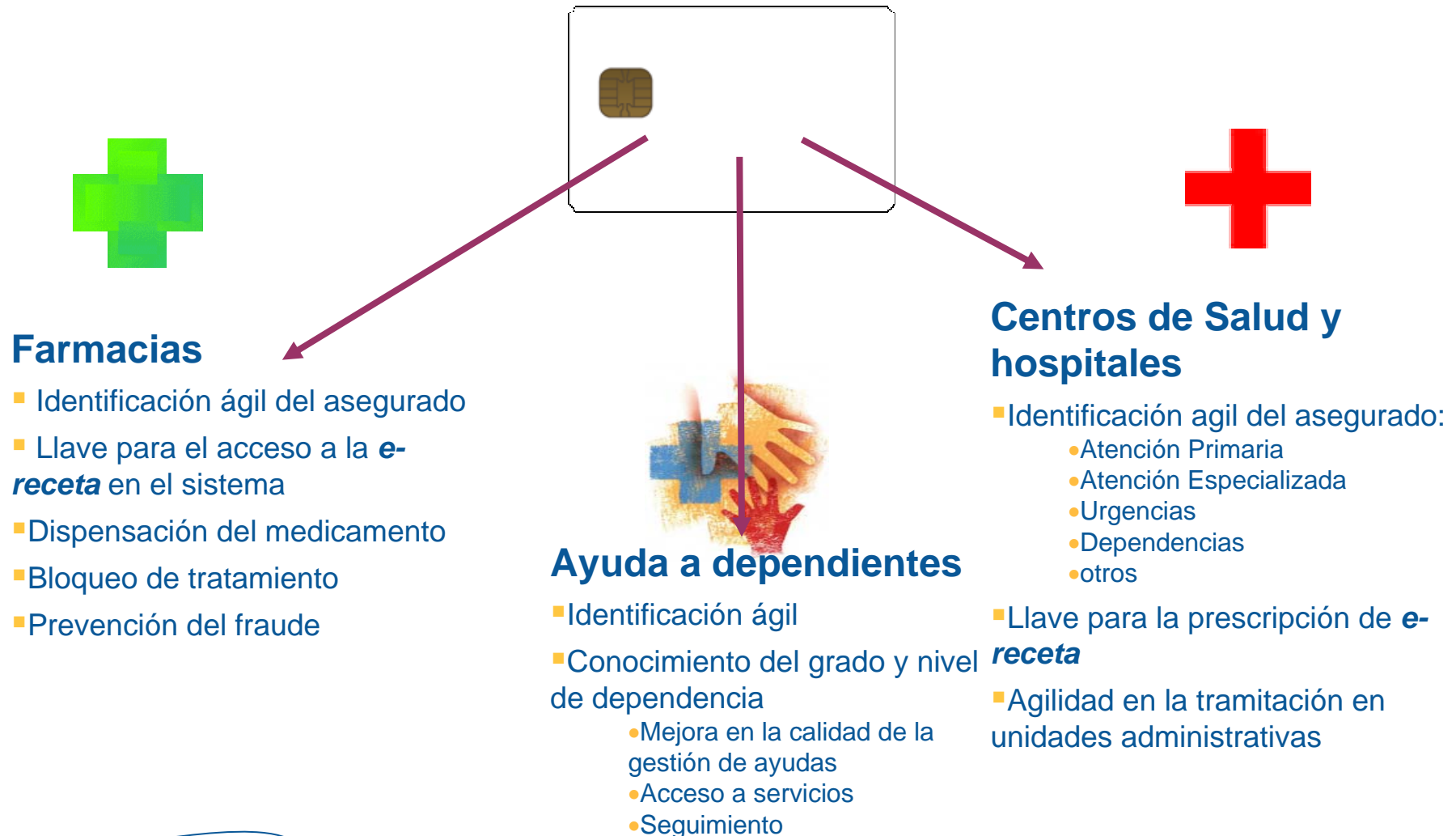


Alcance del proyecto actual

B. de D. de tarjeta CIVITAS



Escenarios de uso de la tarjeta a corto plazo



Decisión sobre la tecnología de la tarjeta: alternativas



Tipo 1: Banda magnética o chip de memoria

- Tarjeta que almacena una pequeña cantidad de información y que es leída/grabada con contacto físico a través de una cabeza lectora/escritora.

Tecnología propietaria
No apta para Internet

Tipo 2: Tarjeta inteligente con criptografía simétrica pero sin posibilidad de tecnología PKI

- Se trata de las tarjetas inteligentes que son capaces de guardar información de forma segura y realizar funciones criptográficas que no impliquen el uso de certificados digitales o firma electrónica

Tecnología propietaria
No apta para Internet

Tipo 3: Tarjeta inteligente criptográfica

- Son tarjetas microprocesadas avanzadas con en las que hay módulos de hardware para la ejecución de algoritmos usados en cifrados simétricos y de clave pública, así como firmas digitales.
- Disponen de un middleware que proporciona interfaces de programación estándar
- Ejemplos de este tipo de tarjeta son: el **eDNI**, así como las tarjetas emitidas por diferentes entidades de certificación públicas: cámaras de comercio, etc.

Tecnología propietaria

Tipo 4: Tecnología JAVA : JAVA Cards

- Son tarjetas con un sistema JVM (Máquina Virtual Java) capaces de ejecutar pequeñas aplicaciones java especialmente diseñadas para el entorno en el que vayan a emplearse
 - (*)Subtipo 4.1.: JAVA sin RSA: sin tecnología PKI
 - (*)Subtipo 4.2.: JAVA con RSA: con tecnología PKI

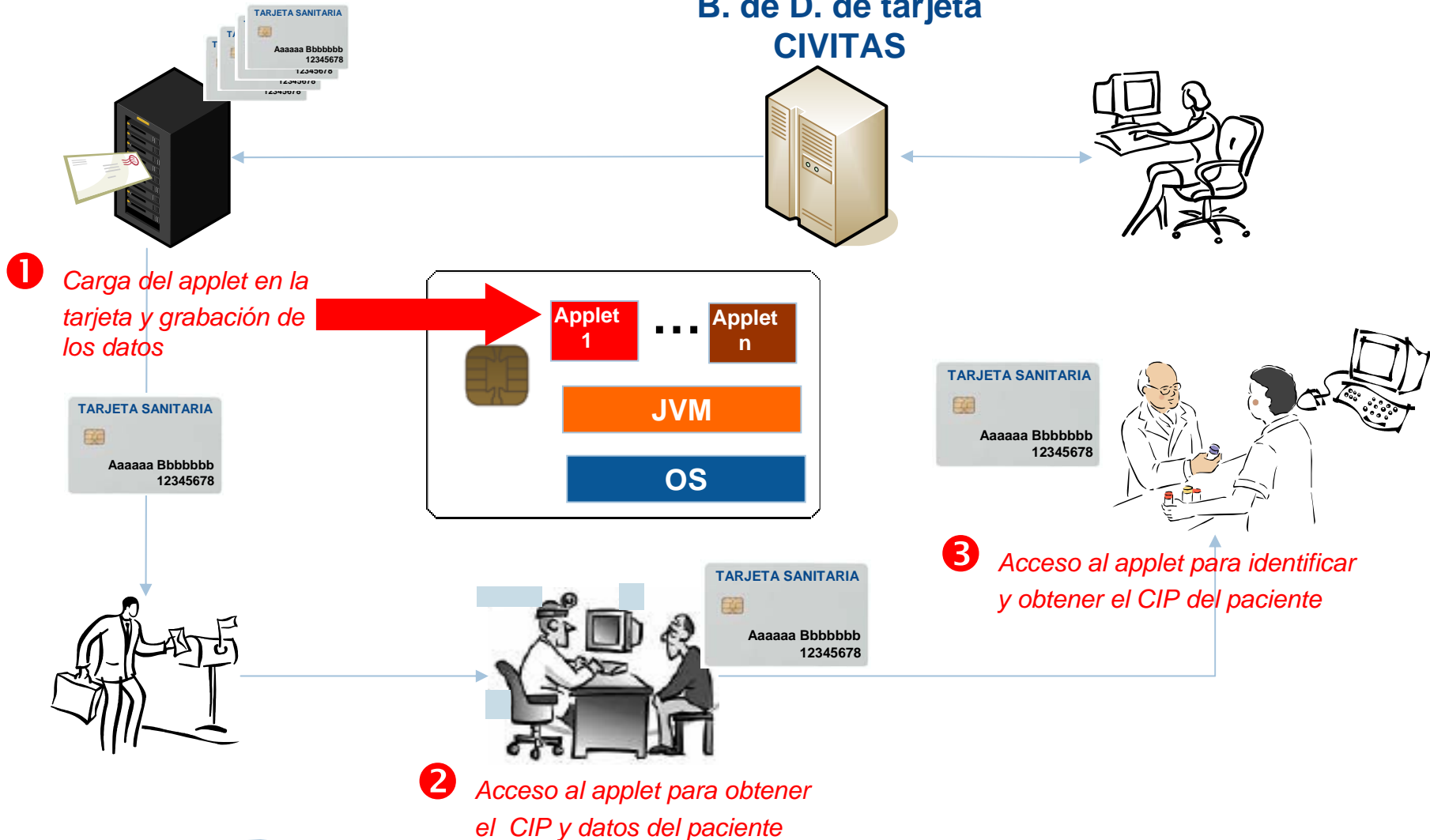
Tecnología elegida

(*) Se realiza esta subdivisión puesto que existe la posibilidad de emplear una tarjeta JAVA sin RSA o con el RSA desactivado mientras no sea necesario.



Applet de acceso a datos

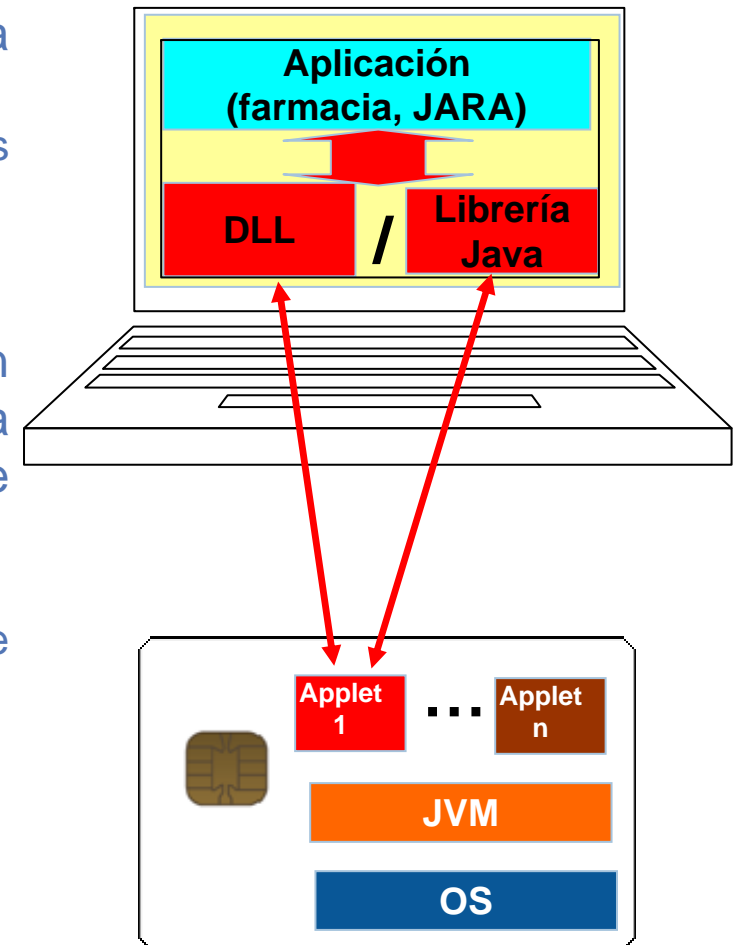
B. de D. de tarjeta CIVITAS



Librerías para la integración en las aplicaciones



- Para cumplir con los requerimientos del proyecto de receta electrónica, los datos en la tarjeta tendrán que ser accedidos por:
 - Los aplicativos que son utilizados en las farmacias para dispensar los medicamentos
 - La aplicación JARA que realiza la prescripción
- Se desarrollarán unas librerías que proporcionen unas APIs de alto nivel para el acceso a la tarjeta, las cuales se pondrán a disposición de las empresas a cargo de la integración
 - Una versión para windows (una DLL)
 - Unas clases Java para Linux con métodos de acceso a la tarjeta



Requisitos de seguridad

- Proteger los datos del asegurado
 - Evitar accesos no autorizados a datos asistenciales
- Prevenir el fraude
 - Impedir la suplantación de identidad: por ejemplo en la dispensación de la receta electrónica



- Asegurar la obligatoriedad de la lectura de la tarjeta en:
 - La dispensación de la receta electrónica
 - En determinados procesos del S.I. asistencial (JARA)



- Autenticación mutua tarjeta-aplicación:
 - Contra la aplicación en la farmacia en la dispensación de la receta electrónica
 - Contra los servicios web de JARA también en el momento de la dispensación (doble verificación)
 - ~~Contra JARA~~ en determinados procesos



Mecanismos de seguridad

1 Generación segura de las claves criptográficas y grabación en las tarjetas

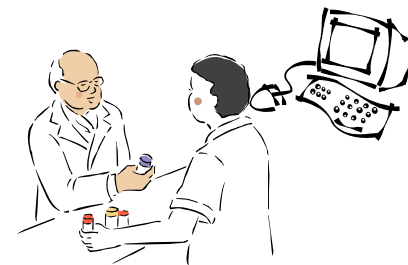


2 Entrega de claves mediante protocolo seguro

S.I. CIVITAS



4 Establecimiento de sesión y autenticación mutua aplicación - tarjeta utilizando K1

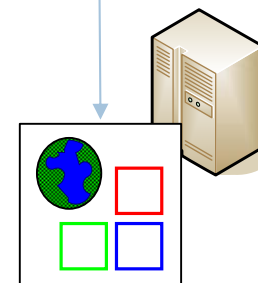


- K1** Clave simétrica 1: tarjeta-farmacia
- K2** Clave simétrica 2: tarjeta-servicios web Jara
- K3** Clave simétrica 3: tarjeta-proceso Jara



3 Establecimiento de sesión y autenticación mutua aplicación - tarjeta utilizando K3
La presencia de la tarjeta sanitaria autoriza el acceso a la Historia Clínica Electrónica

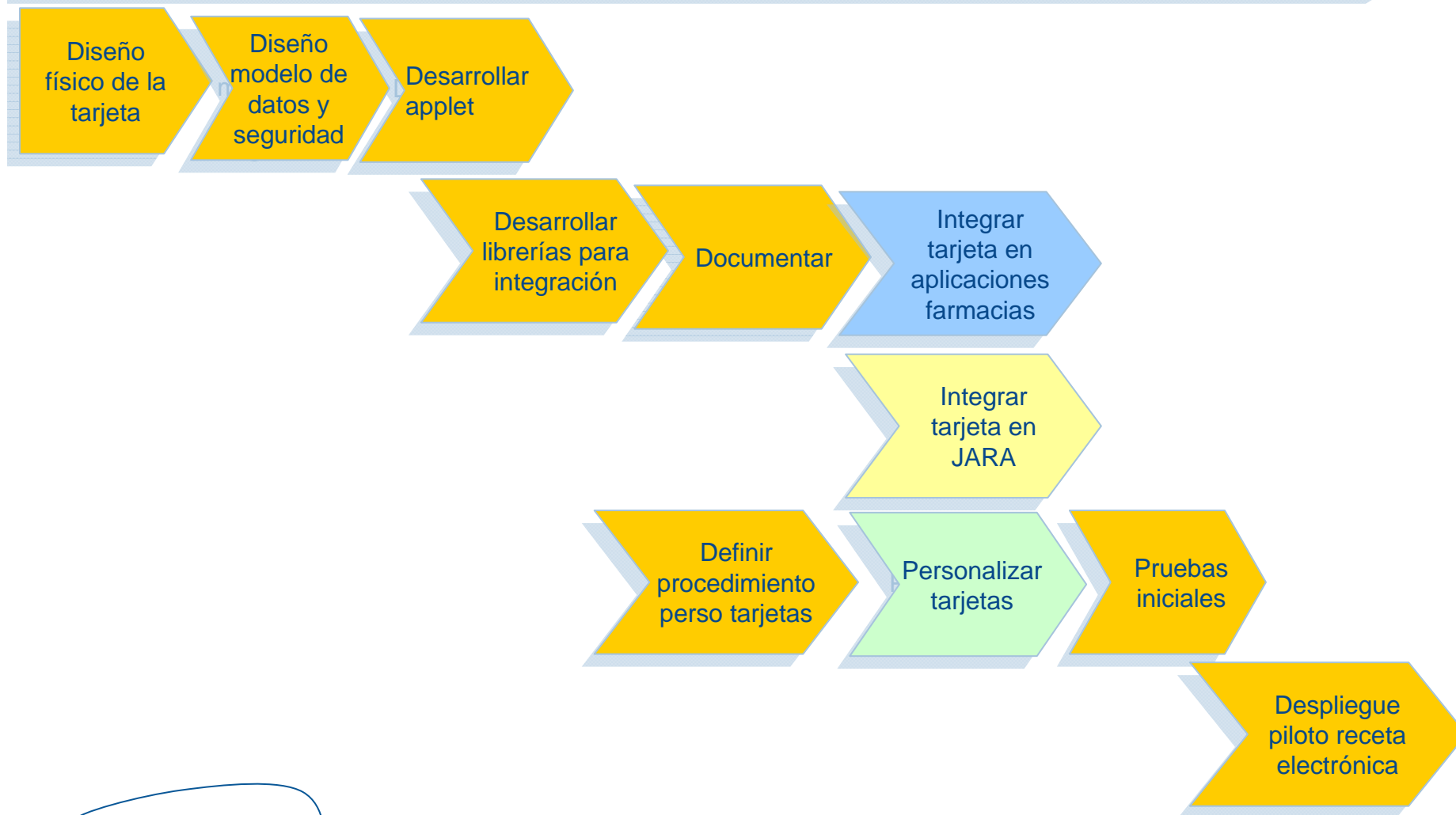
5 Validación contra los servicios WEB de Jara utilizando K2





Coordinación a cargo de una Oficina Técnica

Planificación, coordinación, seguimiento y soporte a cargo de una OFICINA TÉCNICA a cargo de STERIA



The Steria logo is located in the top right corner. It consists of the word "steria" in a dark blue, lowercase, sans-serif font. Below the text is a stylized graphic of a tree branch with three leaves: a pink one on the left, a yellow one in the middle, and an orange one on the right. The entire logo is contained within a white, rounded rectangular shape that has a thin white line extending from its top-left corner across the blue background.

steria

¡ MUCHAS GRACIAS POR SU ATENCIÓN !

eduardo.martin@steria.es