Un estudio del DNIe y de su infraestructura

XVII Reunión Española sobre Criptología y Seguridad de la Información

Javier Correa Marichal, Pino Caballero Gil, Carlos Rosa Remedios, Rames Sarwat-Shaker

/01 Introducción

https://www.cuentafacto.es/tu-interes/para-que-sirve-dni-electronico-como-activarlo/

/01 Introducción

GOBIERNO DE ESPAÑA · MINISTERIO DEL INTERIOR · POLICÍA NACIONAL

POLICÍA NACIONAL

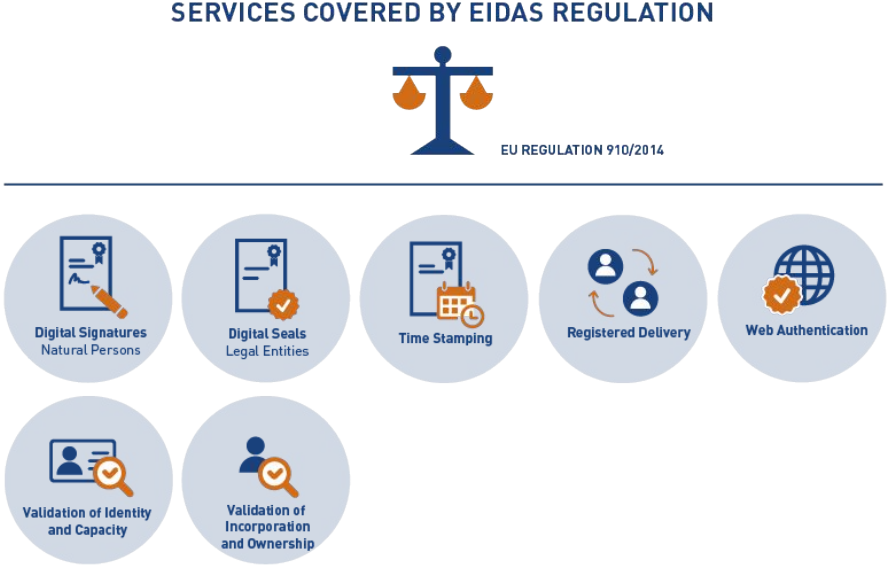
NUEVO DNIe 4.0 – FORMATO EUROPEO

El próximo 2 de agosto de 2021 deberán los países miembros de la UE cumplir con el Reglamento UE 2019/1157 del Parlamento Europeo y del Consejo de 20 de junio de 2019 sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación, que forma parte del Plan de acción 2016 de la Comisión para abordar el fraude de los documentos de viaje, incorporando medidas de seguridad de los documentos como las tarjetas de identidad y de residencia.

Con un plazo de 2 meses de antelación a la fecha señalada, España ya cumple con los criterios establecidos en este Reglamento europeo, facilitando progresivamente a todos los ciudadanos el nuevo formato europeo de DNI electrónico 4.0, que además de incorporar todas las medidas de seguridad y de usabilidad del anterior formato 3.0, tiene un nuevo diseño del propio soporte, añadiendo básicamente los siguientes

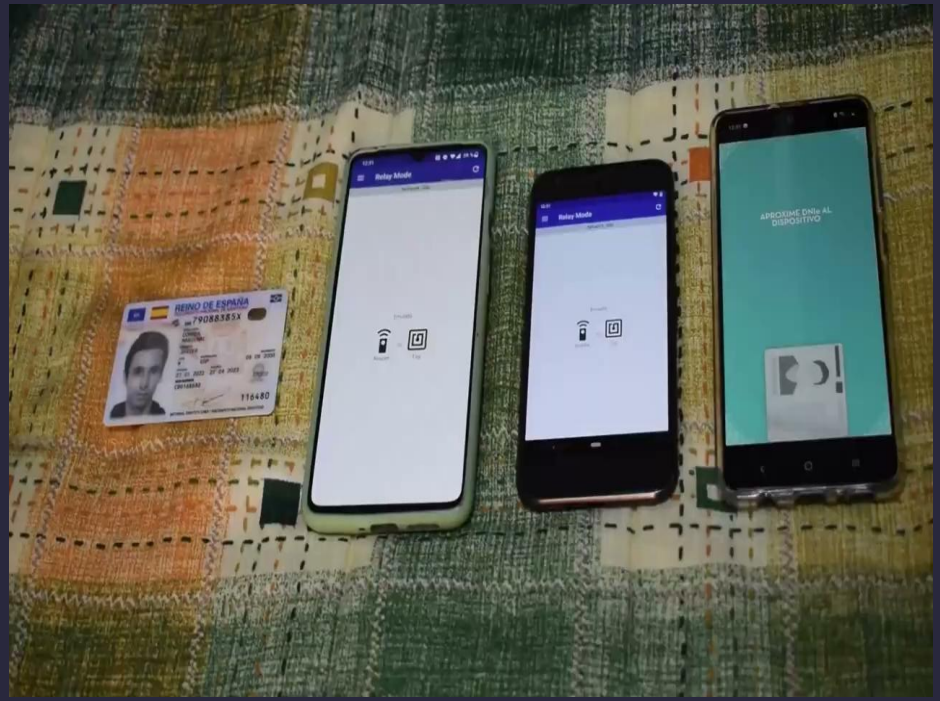
https://www.dnielectronico.es/PDFs/DNI_4.0.pdf

/01 Introducción



/01 Introducción

/02 Ataque de relay



/02 Ataque de relay

Contramedidas:

- Restricciones geográficas
- Restricciones temporales

Y. Hu, A. Perrig and D. B. Johnson, “Wormhole Attacks in Wireless Networks”, IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370-380, 2006

/03 Firma arbitraria de documentos

README.md

Cliente @firma

El Cliente @firma es uno de los productos de la Suite @firma de soluciones de identificación y firma electrónica. Se proporciona de a las Administraciones Públicas para que dispongan de los instrumentos necesarios para implementar la autenticación y firma electrónica avanzada de una forma rápida y efectiva.

El cliente de firma es una herramienta de firma electrónica en entornos de escritorio y dispositivos móviles, que funciona en forma de Applet de Java integrado en una página Web mediante JavaScript, como aplicación de escritorio, o como aplicación móvil, dependiendo del entorno del usuario.

Es software libre con licencia GPL 2+ y EUPL 1.1. Puede consular más información y el código del producto en la forja del CTT.

Construcción del Cliente @firma

Los módulos del Cliente @firma se encuentran preparados para su compilación y empaquetado mediante Apache Maven. A continuación se indican los distintos parámetros a utilizar para construir sus artefactos según el uso que se desee dar.

A cualquiera de los comandos que se indican se le puede agregar el parámetro `-DskipTests` para omitir los tests JUnit.

Módulos básicos y servicios

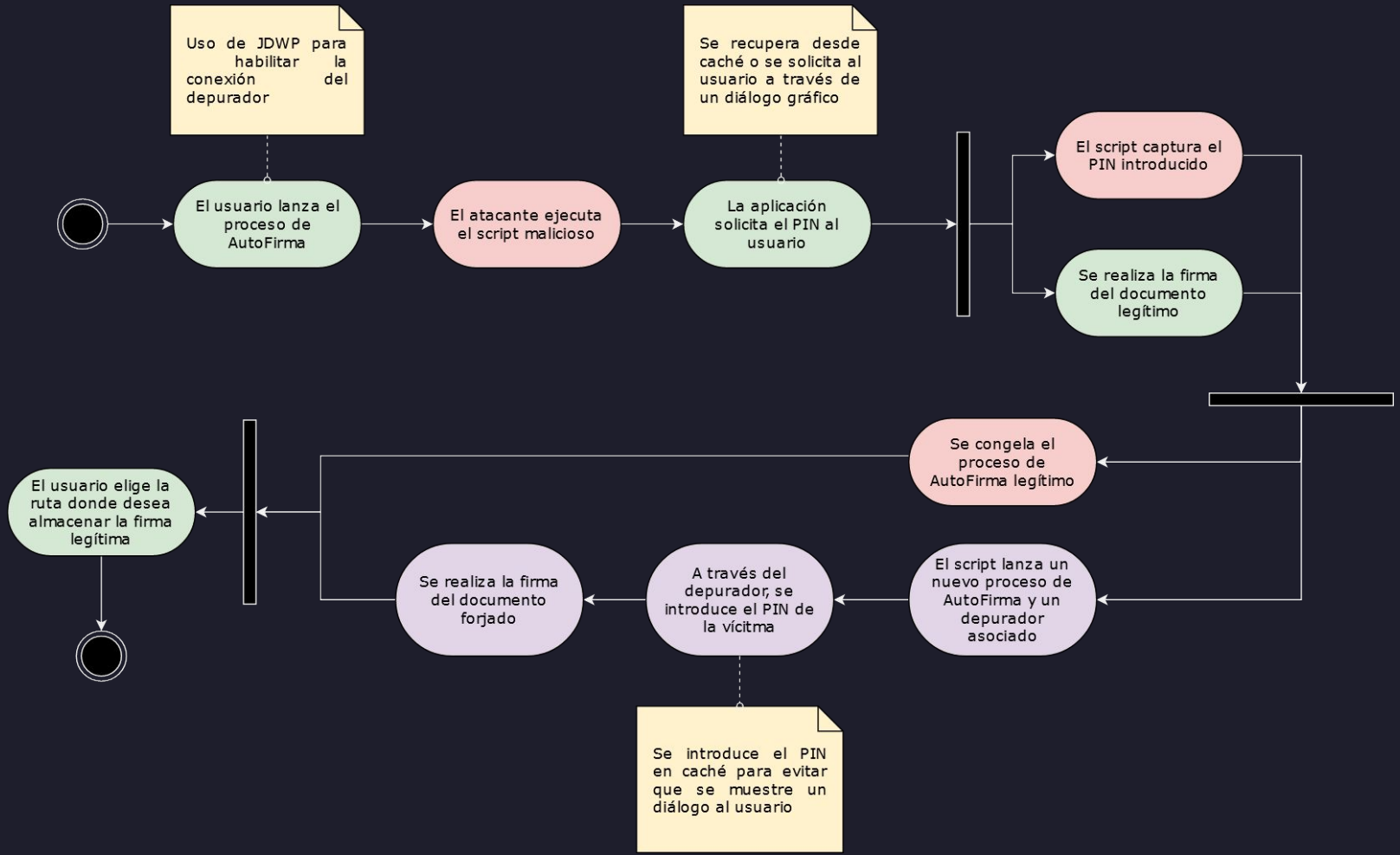
Los módulos del Cliente @firma incluidos en este repositorio se pueden construir mediante el siguiente comando de Maven.

```
mvn clean install
```

Este comando generará todos los módulos básicos del proyecto y los distintos servicios WAR:

/03 Firma arbitraria de documentos

/03 Firma arbitraria de documentos


Uso de JDWP para habilitar la conexión del depurador
Se recupera desde caché o se solicita al usuario a través de un diálogo gráfico
El usuario lanza el proceso de AutoFirma
El atacante ejecuta el script malicioso
La aplicación solicita el PIN al usuario
El script captura el PIN introducido
Se realiza la firma del documento legítimo
Se congela el proceso de AutoFirma legítimo
El usuario elige la ruta donde desea almacenar la firma legítima
Se realiza la firma del documento forjado
A través del depurador, se introduce el PIN de la vícitma
El script lanza un nuevo proceso de AutoFirma y un depurador asociado
Se introduce el PIN en caché para evitar que se muestre un diálogo al usuario

Uso de JDWP para la habilitar la conexión del depurador

Se recupera desde caché o se solicita al usuario a través de un diálogo gráfico

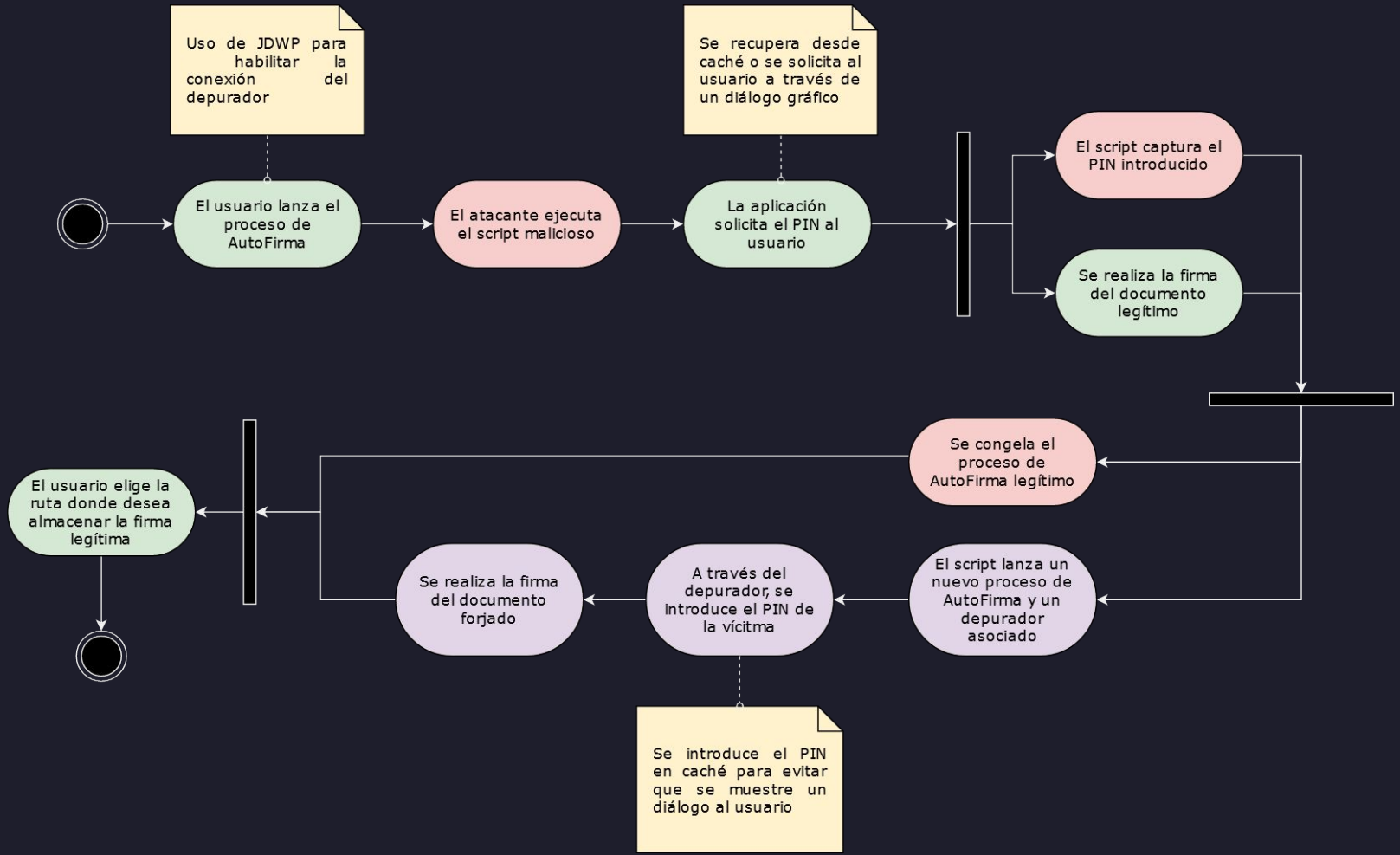
```
~/Desktop/RECSI/AutoStealer main ?1 ❯ which AutoFirma
/usr/bin/AutoFirma

~/Desktop/RECSI/AutoStealer main ?1 ❯ export PATH=$(pwd):$PATH

~/Desktop/RECSI/AutoStealer main ?1 ❯ which AutoFirma
/home/zodi4c/Desktop/RECSI/AutoStealer/AutoFirma

~/Desktop/RECSI/AutoStealer main ?1 ❯ cat AutoFirma
```

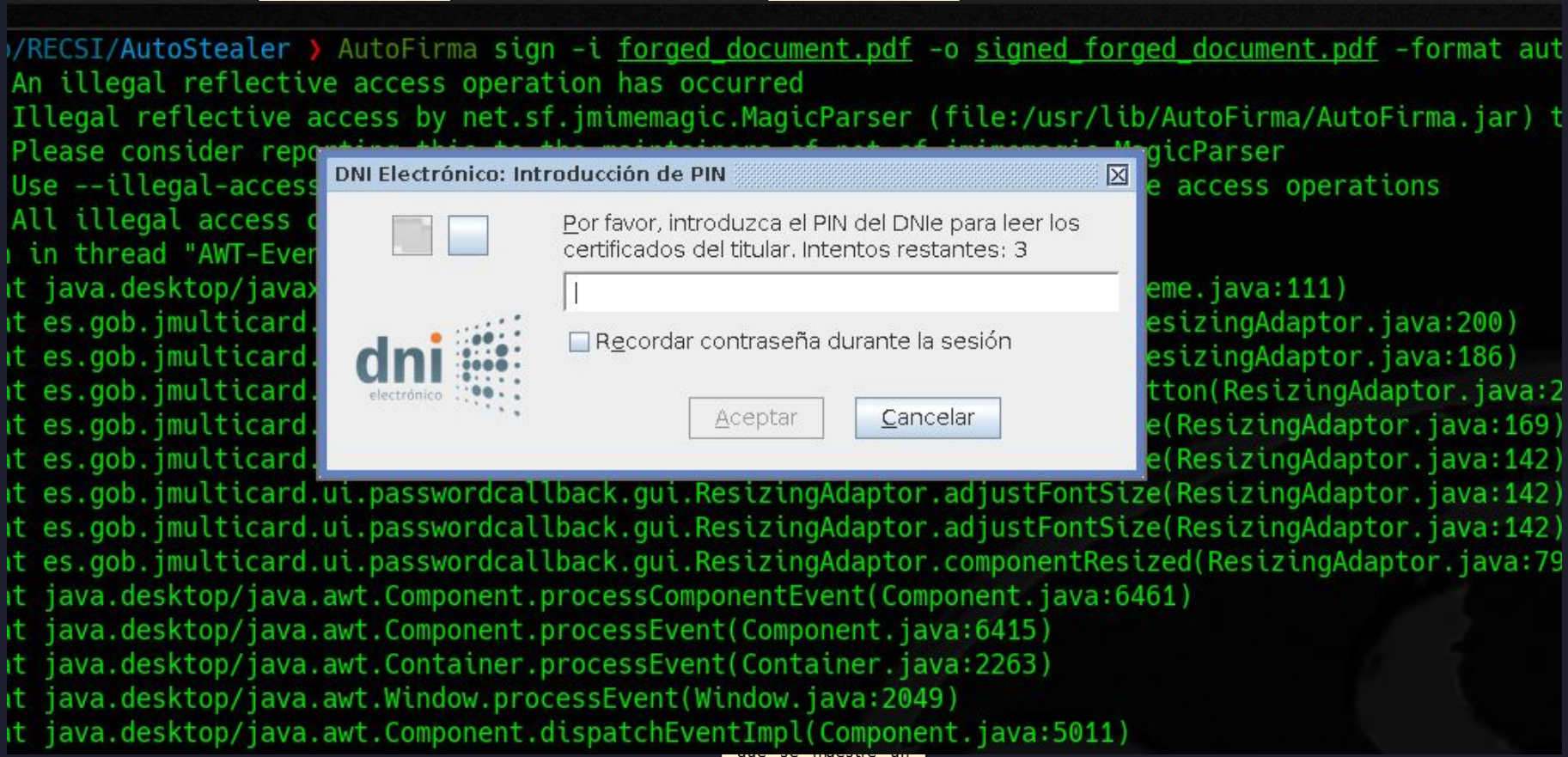
File: AutoFirma

```
1  #!/bin/bash
2  java -agentlib:jdwp=transport=dt_socket,address=8000,server=y,suspend=n -jar /usr/lib/AutoFirma/AutoFirma.jar $@ |
```

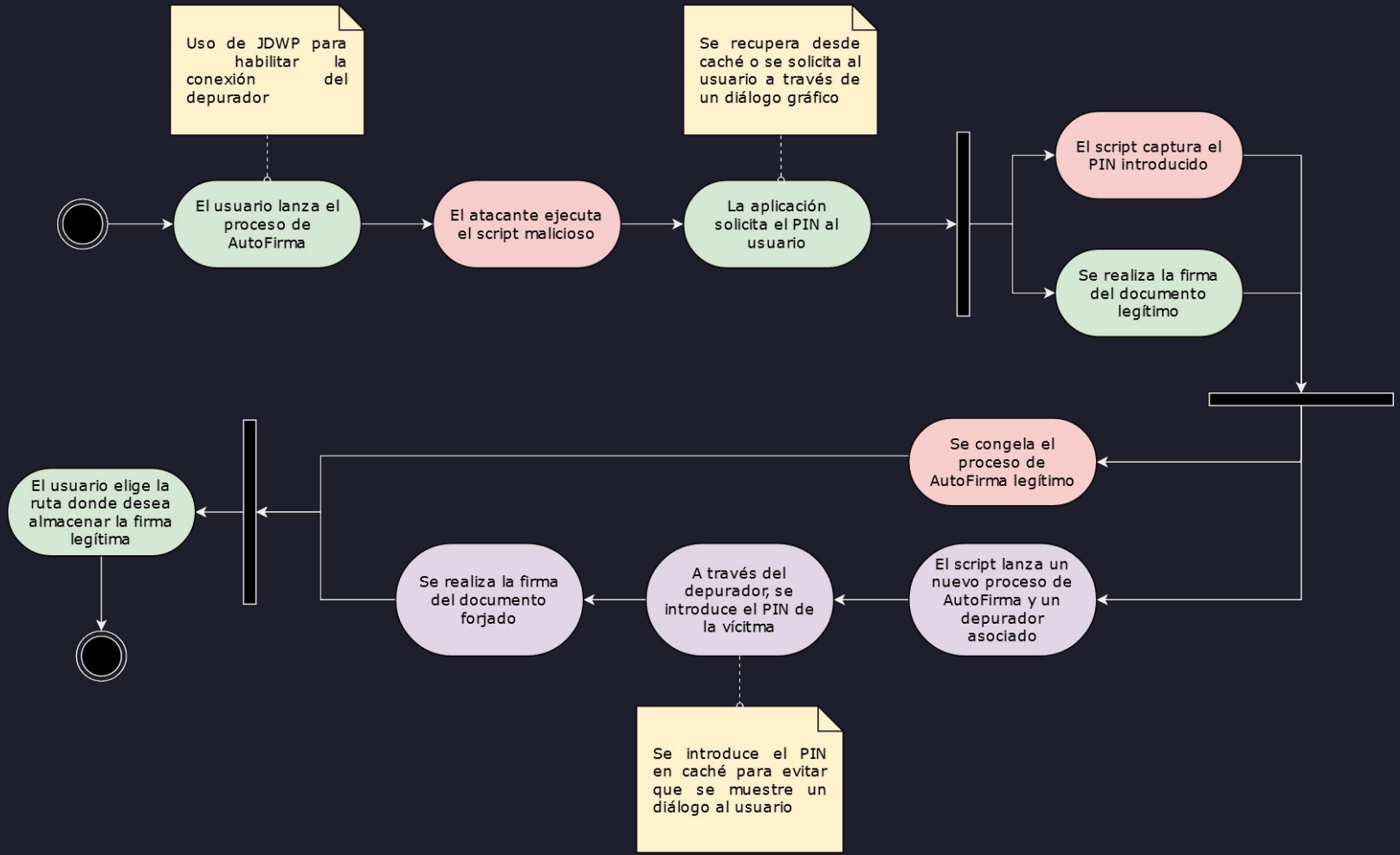
```
~/Desktop/RECSI/AutoStealer main ?1 ❯
```

Se introduce el PIN en caché para evitar que se muestre un diálogo al usuario


Uso de JDWP para habilitar la conexión del depurador
Se recupera desde caché o se solicita al usuario a través de un diálogo gráfico
El usuario lanza el proceso de AutoFirma
El atacante ejecuta el script malicioso
La aplicación solicita el PIN al usuario
El script captura el PIN introducido
Se realiza la firma del documento legítimo
Se congela el proceso de AutoFirma legítimo
El usuario elige la ruta donde desea almacenar la firma legítima
Se realiza la firma del documento forjado
A través del depurador, se introduce el PIN de la vícitma
El script lanza un nuevo proceso de AutoFirma y un depurador asociado
Se introduce el PIN en caché para evitar que se muestre un diálogo al usuario

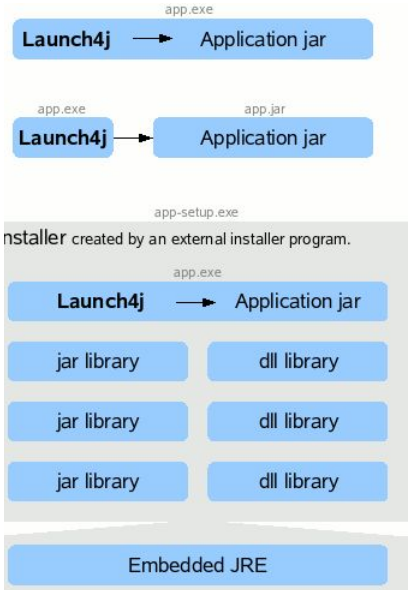


diálogo al usuario


Uso de JDWP para habilitar la conexión del depurador
Se recupera desde caché o se solicita al usuario a través de un diálogo gráfico
El usuario lanza el proceso de AutoFirma
El atacante ejecuta el script malicioso
La aplicación solicita el PIN al usuario
El script captura el PIN introducido
Se realiza la firma del documento legítimo
Se congela el proceso de AutoFirma legítimo
El usuario elige la ruta donde desea almacenar la firma legítima
Se realiza la firma del documento forjado
A través del depurador, se introduce el PIN de la vícitma
El script lanza un nuevo proceso de AutoFirma y un depurador asociado
Se introduce el PIN en caché para evitar que se muestre un diálogo al usuario

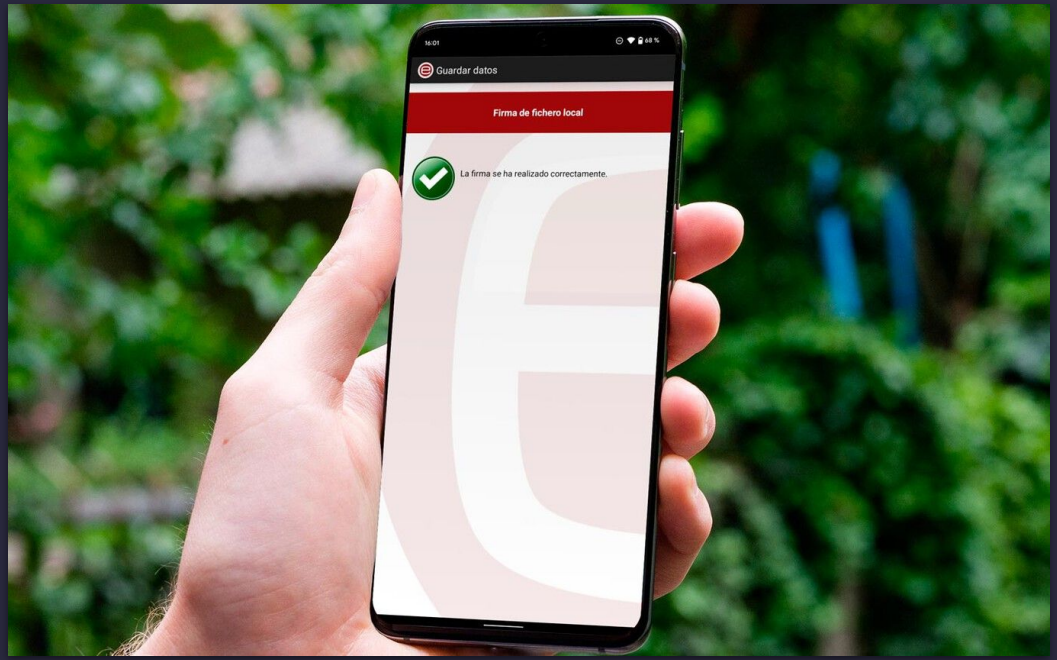
/03 Firma arbitraria de documentos

launch4j



https://launch4j.sourceforge.net

/04 Conclusiones



https://www.xatakandroid.com/tutoriales/autofirma-para-android-asi-puedes-firmar-documentos-oficiales-directamente-movil

¡GRACIAS!

¿Preguntas?