

# Identidad digital móvil



**III International Congress**  
University Smart Card

# Identidad digital: Antecedentes

Tradicionalmente la identidad digital se acredita con el uso de usuario/contraseña.

Inconvenientes:

- Mecanismos poco seguros
- Dificultad de gestión para el usuario
- No se generan evidencias electrónicas
- No apto para la mayoría de relaciones telemáticas con administraciones

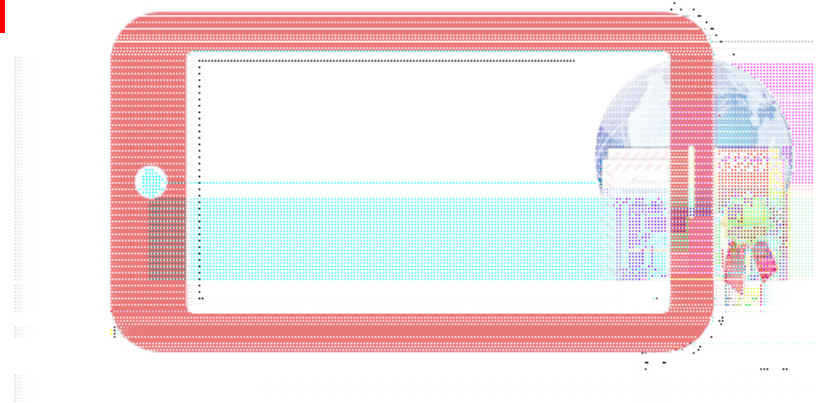
# ¿Cómo reforzar la seguridad?



La manera óptima de asegurar la identidad y actuación digital es a través de los certificados electrónicos, pero debemos tener en cuenta:

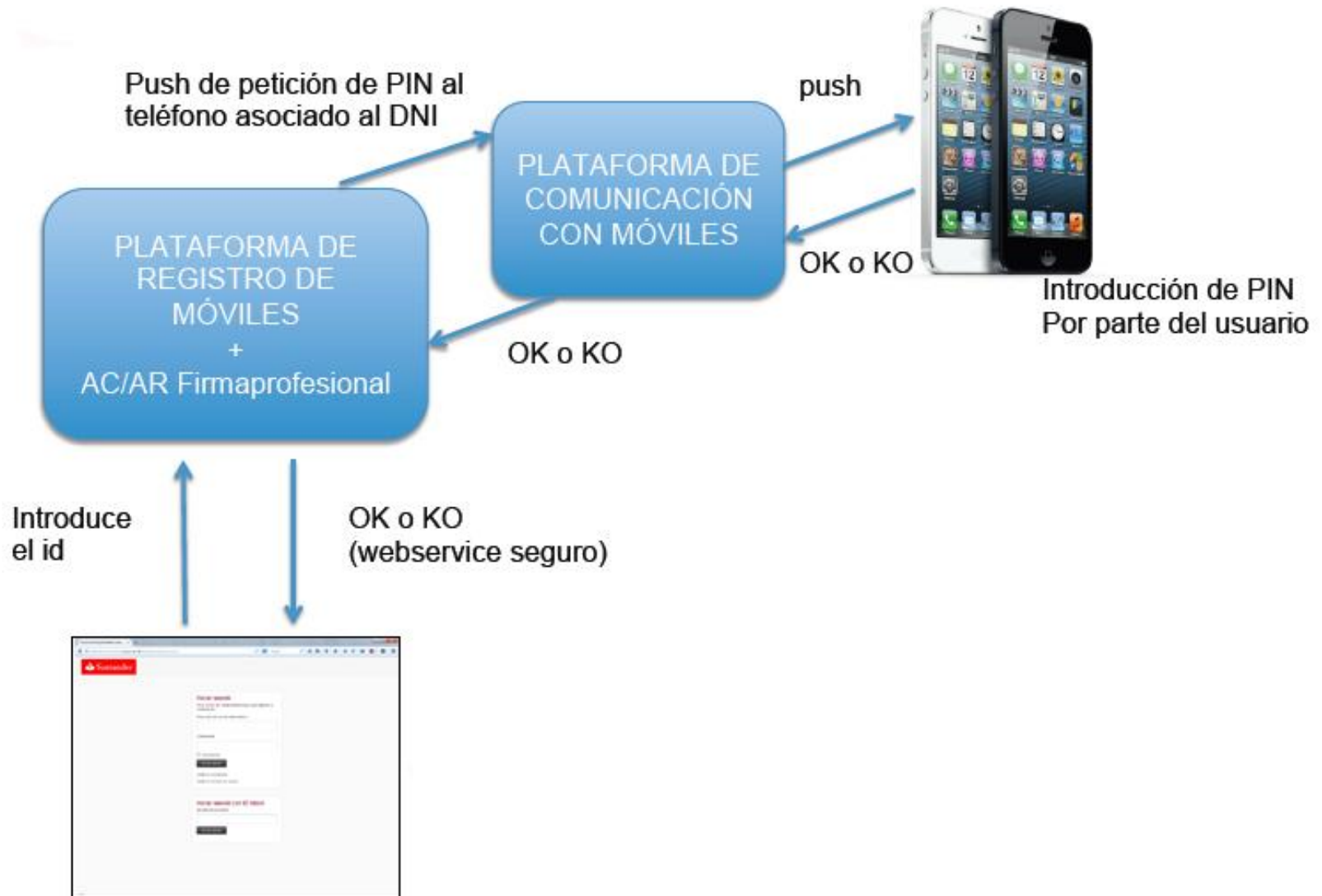
- No son fáciles de utilizar en algunos ámbitos.
- Los dispositivos criptográficos necesitan adaptación a los equipos del usuario.
- El acceso a la red con smartphones se está extendiendo rápidamente, se hace necesario establecer una mayor seguridad.

## Solución: Identidad digital móvil



- Utiliza como medio el dispositivo digital de uso masivo hoy: el móvil.
- Experiencia de usuario natural, sin visualizar el certificado digital.
- Creación de las evidencias electrónicas necesarias en relaciones telemáticas.
- Máxima usabilidad.
- Provee funciones de autenticación segura y firma electrónica avanzada.

# ¿Cómo funciona?





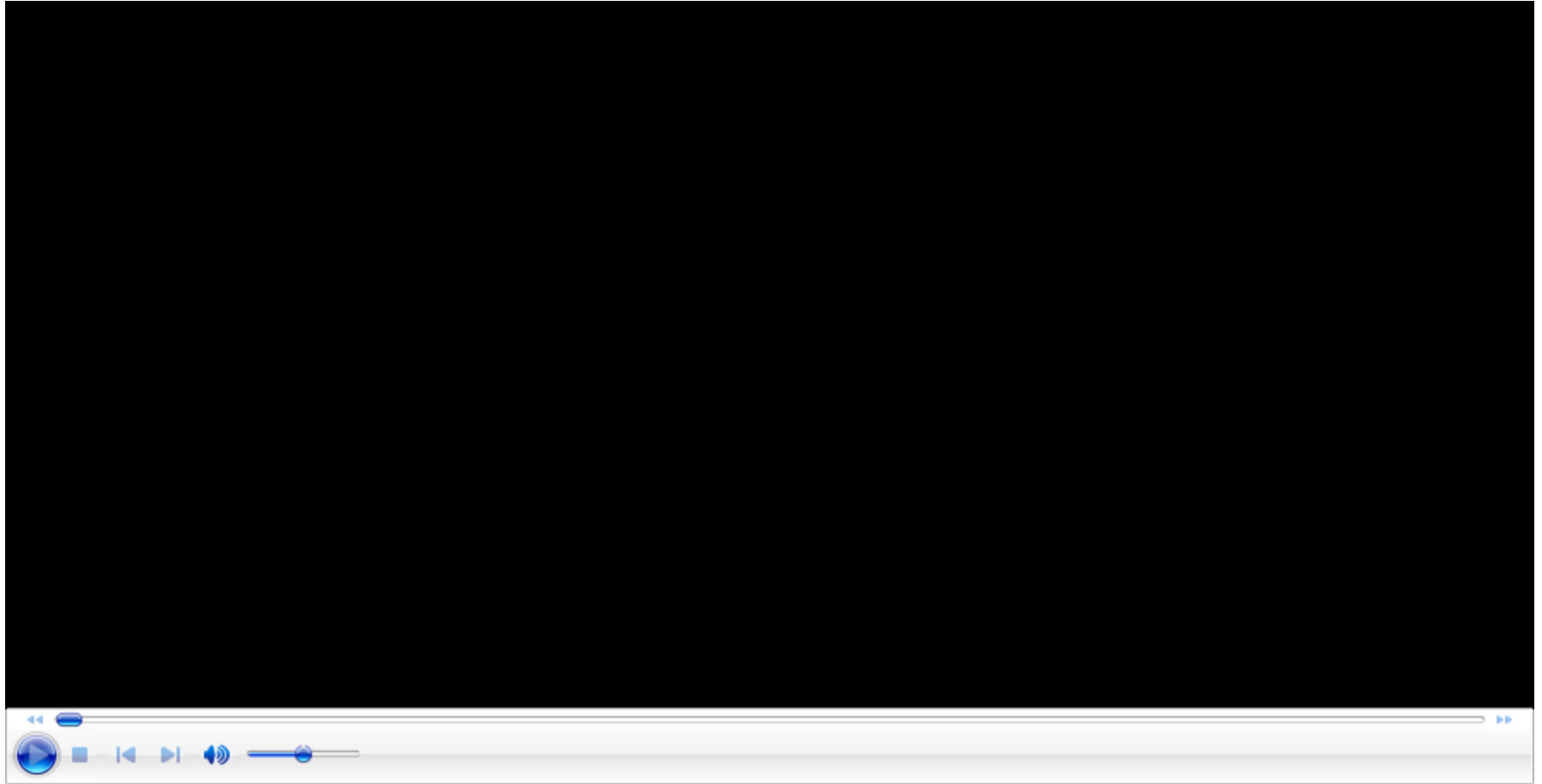
- Registro de móviles basado en identificación presencial, protegido con seguridad fuerte (de autoridad de registro).
- El par de claves se generan en el dispositivo móvil y la clave privada no sale del sandbox de la App.
- Despliegue de capacidad de autenticación y firma electrónica avanzada basada en certificado reconocido.
- En el futuro (elemento seguro en móvil) permite la evolución natural a firma reconocida.

# Alta en el sistema

- Procedimiento intuitivo
- PIN propio de la app, no es necesario que sea el mismo que el de la SIM
- Varios niveles de acreditación:
  1. Registrado: el usuario aún no ha acreditado su identidad de forma presencial
  2. Acreditado: La oficina de registro ya ha comprobado la identidad del usuario

## Ejemplo de uso: Alta

En la siguiente demo se puede observar el proceso de registro inicial del usuario en la aplicación:





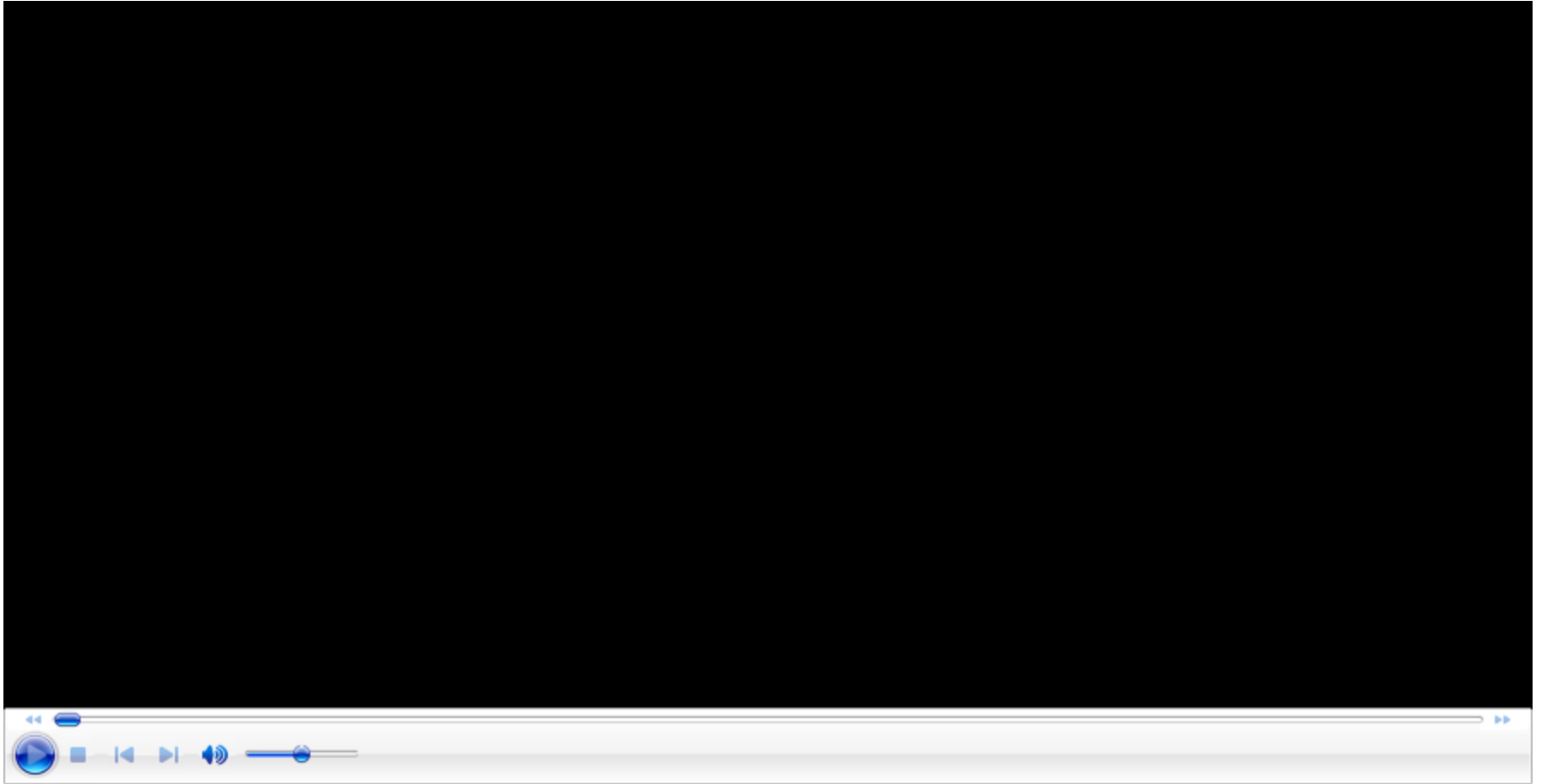
# Autenticación segura



- El procedimiento de login con la operativa tradicional, introduciendo usuario y password está expuesta a diferentes riesgos:
  - Phishing
  - Keyloggers
  - Ataques por fuerza bruta
- Utilizando el ID móvil, el usuario solo introduce su ID en la máquina desde la que desea acceder, la validación se realiza en su móvil marcando el PIN de la app.

## Ejemplo de uso: Autenticación

En la siguiente demo se realiza el login en una misma página con las dos opciones comentadas: operativa tradicional (usuario/password) y con ID móvil:

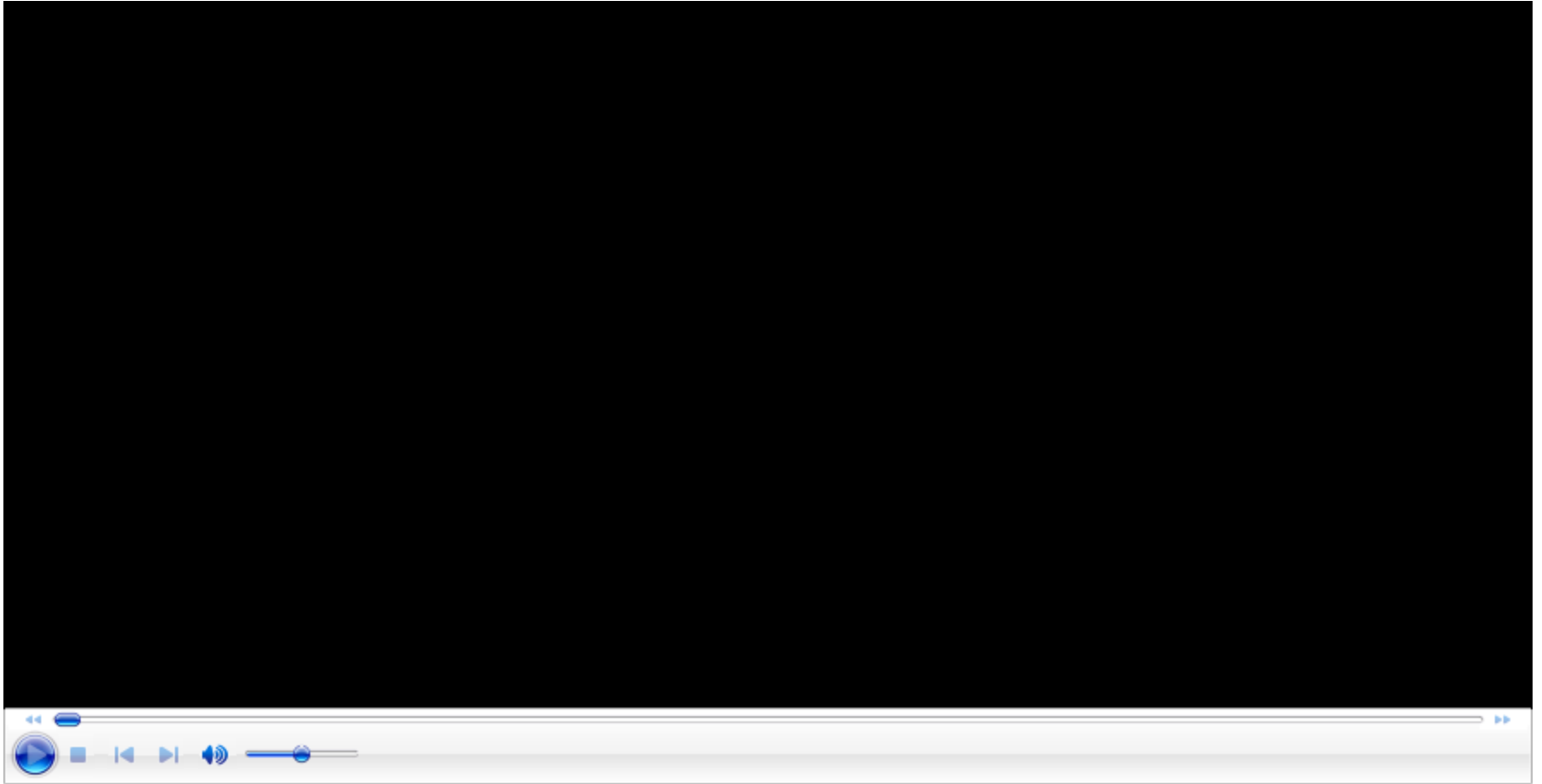


# Firma electrónica

- Simplifica el uso de la firma electrónica para el usuario
- Elimina la problemática de instalación de drivers, middleware, etc.
- Posibilita el registro datos de geolocalización de cada operación

## Ejemplo de uso: Firma electrónica

En el siguiente vídeo se observa el proceso de firma de un documento desde el Móvil:





- Función de firma electrónica móvil
- Piloto Universidad Técnica Federico Santa María
  - Mejora del sistema de recuperación de contraseñas
  - Seguridad adicional en registro del acta de notas

# Próximamente

- Integración en AppTUI
- Interacción con la TUI como elemento seguro
- Mejoras en usabilidad
- Uso de ID móvil en otras aplicaciones del Santander

# Caso de éxito: Ayuntamiento de Barcelona



mobileID  
La identidad digital ciudadana en el móvil

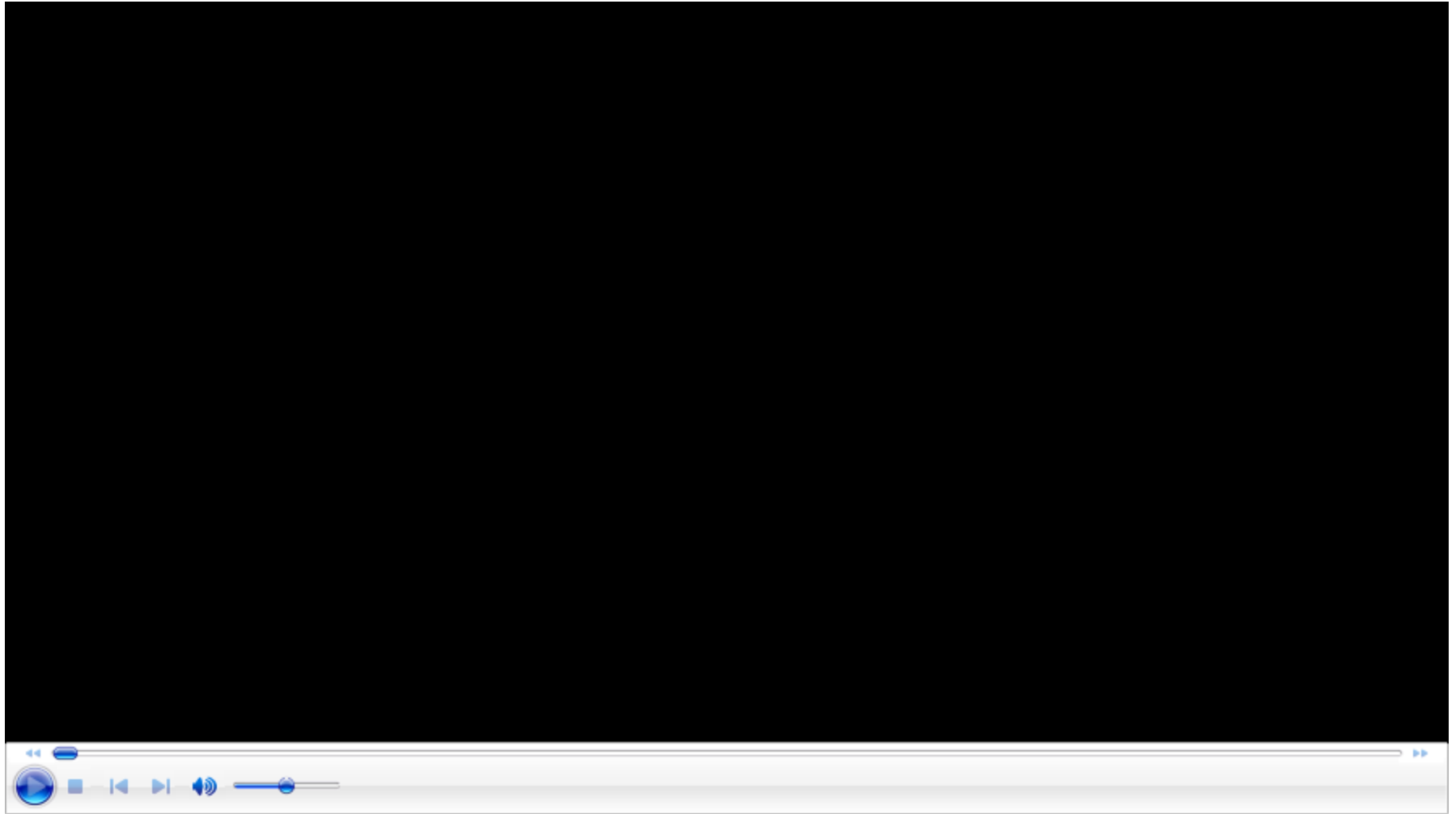


## Servicios disponibles:

- Cita con el Ayuntamiento de Barcelona
- Acceso a carpeta ciudadana
- Solicitud de volante de empadronamiento
- Pago de impuestos y multas
- Información sobre grúa municipal
- Consulta previa para la tramitación de expedientes de obras

# Caso de éxito: Ayuntamiento de Barcelona

Vídeo promocional del proyecto:





Pedro Lara: [pedro.lara@servexternos.isban.es](mailto:pedro.lara@servexternos.isban.es)

Juan Carlos Martínez: [jmartivi@isban.es](mailto:jmartivi@isban.es)

