FICHA TÉCNICA

Mobile ID Smart App de Gemalto

RESUMEN DE MOBILE ID SMART APP DE GEMALTO

- **Aborda el desafío de combinar seguridad y usabilidad**
- **Tecnología probada en el campo, confiable en todo el mundo**
- **Solución inclusiva que funciona en todos los teléfonos inteligentes**
- **Admite la autenticación biométrica para brindar facilidad de uso a lo largo de la experiencia de autenticación**
- **Ofrece una experiencia de incorporación remota fluida desde múltiples canales**
- **Construida según principios de privacidad desde el diseño; basada en el consentimiento y dando a los usuarios el control de sus datos**
- **Permite al usuario final firmar digitalmente los datos usando la clave privada que reside en el teléfono inteligente**
- **Puede convertirse en un lector de documentos electrónicos NFC para ofrecer capacidades de firma electrónica legalmente reconocidas**
- **Proporciona el más alto nivel de seguridad en el mercado**
- **Seguridad de software móvil mejorada, basada en el Mobile Security Core**
- **Resistente a los ataques de malware más virulentos y al acceso no autorizado**
- **El almacenamiento seguro encriptado incorporado utiliza una criptografía sólida para mantener los datos seguros y protegidos en todo momento**
- **Desarrollada por la plataforma back-end de servicios de identidad digital de Gemalto**

Descripción del producto

La aplicación inteligente de identidad móvil de Gemalto Mobile ID Smart App se introdujo para cumplir con los crecientes requisitos del mercado de contar con una experiencia avanzada de usuario de teléfono inteligente para servicios en línea que no comprometa la seguridad. La aplicación permite a los ciudadanos autenticarse en sitios web, confirmar transacciones y realizar firmas electrónicas con conveniencia y facilidad. Almacena la identidad digital del usuario móvil y garantiza que sus credenciales digitales estén protegidas y seguras en todo momento.

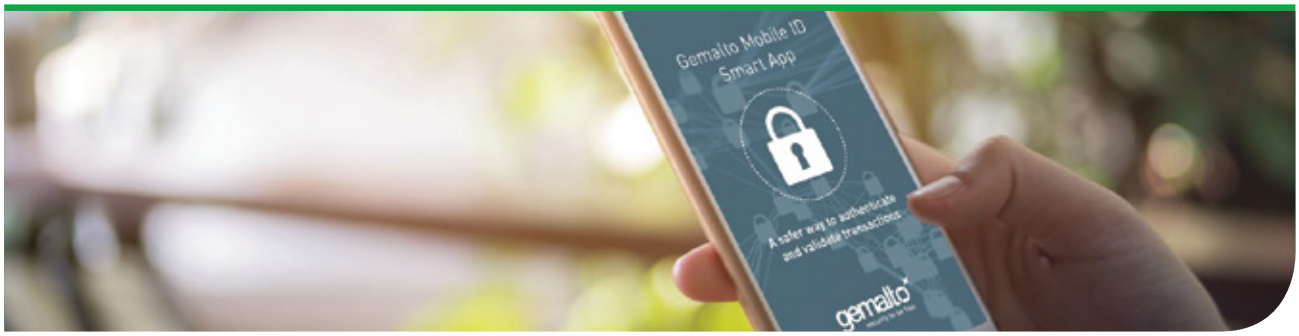
Modelo de despliegue

- Disponible como app o como kit de desarrollo de software (SDK)
- Gemalto Mobile ID Smart App: IU personalizable con branding específico (visualización y logo) para cumplir con las pautas y la localización del cliente en cuanto al idioma de preferencia.
- Gemalto Mobile ID Smart SDK: permite una integración simple de las características de Gemalto Mobile ID Smart en la aplicación de cualquier cliente

Seguridad

- Comunicación fuera de banda para mitigar los riesgos de un solo canal
- Basado en Gemalto Mobile Security Core con protección avanzada contra malware y dispositivos corruptos
- Ofuscación de código sensible para proteger contra la ingeniería reversa y el hackeo
- Protección RASP
  - Detección de Jailbreak/Root
  - Detección de herramientas de ocultación de Jailbreak/Root
  - Anti-hooking
  - Anti-depuración
  - Anti-manipulación estática
  - Anti-emulador
  - Anti-manipulación dinámica
- El teclado PIN seguro de Gemalto permite un diseño aleatorizado y elimina la necesidad de almacenar el valor del PIN en la memoria RAM del dispositivo
- Políticas configurables de validez de PIN (por ejemplo, no uniformidad, sin orden ascendente/descendente, sin combinaciones prohibidas, etc.)
- Almacenamiento encriptado seguro
  - Utiliza cifrado asimétrico para proteger las claves y las credenciales
  - Las claves de cifrado están diversificadas por huellas dactilares de aplicaciones y dispositivos, y están protegidas por PIN

Ficha técnica - Mobile ID Smart App de Gemalto



Comunicación

> Comunicación segura basada en CP/IP con la plataforma *back-end* de servicio de identidad digital de Gemalto
> Utiliza protocolo TLS y la comunicación adicional cifrada y segura de punta a punta
> Claves de sesión e integridad para una comunicación segura generadas para cada solicitud y eliminadas al recibir la respuesta
> Se comunica con mensajes push o mediante el sondeo del *back-end* para recibir la solicitud

Experiencia del usuario

> Soporta una amplia gama de métodos de autenticación
  • PIN, patrón, facial con detección de prueba de vida, huella dactilar Electrónica Cualificada (QES) eIDAS
> El usuario puede cambiar de un método de autenticación a otro
> Registro y navegación de las operaciones principales
> Soporte multidispositivo

Plataforma *back-end*

> Gestionado por la plataforma *back end* de servicios de identidad
digital de Gemalto (registro del usuario final, asociación de dispositivo, generación de claves PKI, autenticación, procesos de firmas, etc.)
> Autenticación usando SAML 2.0, Open ID Connect 2.0
> Firma usando OASIS DSS, compatible con la firma electrónica cualificada (QES) de eIDAS
> Compatible con el GDPR – basado en la minimización de datos, en la protección de datos, en la seudonimización, en la anonimización, en la gestión de los datos y en el consentimiento del usuario
> Portales de autogestión y atención al cliente / API para la gestión del ciclo de vida de la aplicación inteligente de identidad móvil

Enrolamiento

> Admite la prueba de identidad remota mediante:
  • Documentos electrónicos basados en eID, ICAO
  • Documentos de identidad no electrónicos
> Identificación biométrica
> Escaneo de código QR o registro basado en URL

Autenticación

> Mobile ID Smart App independiente: eIDAS Substantial, NIST AAL 2, ISO LoA 3
> Mobile ID Smart App + tarjeta eID NFC + PIN: eIDAS High, NIST AAL 3, ISO LoA 4
> Mobile ID Smart App + doc OACI + Reconocimiento facial: eIDAS High, NIST AAL 3, ISO LoA 4

Firma digital

Niveles
Mobile ID Smart App independiente: Firma Electrónica Avanzada (AES) eIDAS
Mobile ID Smart App + tarjeta eID NFC + PIN: Firma

Formatos
> Sign Hash (PKCS#1/CAdES-BES) – Firma de documentos
  • XML (xmlDsign)
  • PDF (binario o XML incorporado en documento PDF)
  • ASIC - Firma asociada al contenedor zip

> Sign Text (PKCS#7/CMS/CAdES-BES) – Firma de texto

Características de gestión de claves

> Generación de claves a bordo (OBKG): generada en la app mediante un motor criptográfico, guardada en el almacenamiento seguro cifrado de la aplicación
> Registro y solicitud de certificación Mobile PKCS#10
> Soporta múltiples claves

Criptografía

> RSA: clave de 2048-bit y más
> ECC: ECDSA clave de 256-bit y más
> SHA-256, SHA-512

Sistema Operativo móvil cubierto por defecto

> Android 5.0 y posteriores
> iOS 10.0 y posteriores

Ficha técnica - Mobile ID Smart App de Gemalto

Funcionalidad de valor agregado como opciones

Combinación de identidad móvil y documentos de identidad electrónicos Funciona

con Gemalto Mobile Link

ESPECIFICACIONES	
Aplicaciones admitidas	ICAO, IAS v 4, eIDAS Token NFC, APDU, PACE
Comunicación	eIDAS High, NIST AAL 3, ISO LoA 4 (eDoc + facial, eID + PIN)
Autenticación	Tarjeta eID PKI, Firma electrónica Cualificada eIDAS
Firma digital Prueba de identidad	eIDAS High, NIST IAL 3 (eDoc + facial, eID + PIN)

Combinación de identidad móvil y documentos de identidad no electrónicos

Funciona con la solución de verificación de identidad remota de Gemalto

ESPECIFICACIONES	
Tarjetas admitidas	Admite más de 1350 documentos nacionales
Comunicación	Imagen
Prueba de identidad	eIDAS Substantial, NIST IAL 2 (Imagen de documento + facial)

Normas y especificaciones

- RSA PKCS#1 v2.1: Estándar de cifrado RSA
- RSA PKCS#7 v1.5: Estándar de sintaxis de mensaje criptográfico
- RSA PKCS#10 v1.7: Estándar de sintaxis de petición de certificado
- RFC 2630: Sintaxis de mensaje criptográfico (CMS)
- RFC 5126: Firmas electrónicas avanzadas CMS (CAdES)
- RFC 5280: X.509 Certificado de infraestructura de clave pública y perfil de lista de revocación de certificados (CRL)
- ETSI TS 102 176-1 Algoritmos y parámetros para firmas electrónicas seguras, Parte 1: Funciones hash y algoritmos asimétricos
- ETSI TR 119 312 Firmas e Infraestructuras Electrónicas (ESI); Conjuntos criptográficas
- ANSI X9.62-2005, Criptografía de clave pública para la industria de servicios financieros: el algoritmo de firma digital de curva elíptica (ECDSA)
- ISO29115 - 2013: marco de aseguramiento de autenticación de entidad
- Reglamento (UE) N° 910/2014 - eIDAS
- Pasaporte de la OACI

ACERCA DE GEMALTO

Gemalto es el líder mundial en seguridad digital con ingresos en 2017 de €3,000 millones. En el sector de la identidad civil, Gemalto proporciona documentos seguros, soluciones y servicios de identidad robustos que se encargan de los programas gubernamentales para la gestión de tarjetas de identidad y la seguridad vial, esquemas e infraestructuras confiables de identidad móvil y digital para servicios electrónicos públicos seguros, y requisitos de gestión de fronteras y visas.
Gemalto también aborda los desafíos de la seguridad pública y de la aplicación de la ley, ofreciendo soluciones forenses de primera clase.

Los productos y las soluciones de la compañía se implementan en más de 200 programas activos en todo el mundo, con experiencia específica en emisión de documentos seguros, biometría, lectores de documentos, autenticación, gestión de identidad y protección de datos. Gemalto colabora con sus clientes para informar y compartir las mejores prácticas.

GEMALTO.COM/LATAM

gemalto
security to be free