Mobile Security Core de Gemalto

Estableciendo las bases confiables necesarias para permitir que tanto Mobile ID Smart App (la aplicación inteligente de identidad móvil) de Gemalto como la cartera más amplia de Digital ID Document Wallet detecten la amenaza del malware móvil, y reaccionen y se protejan contra él.

¿Para qué sirve?

La accesibilidad es clave para el éxito y la adopción de los servicios digitales. Por lo tanto, el gran volumen de teléfonos inteligentes en todo el mundo (unos seis mil millones para 2020, según la investigación de mercado de IHS) ofrece a los gobiernos una gran oportunidad para proporcionar a los ciudadanos una identidad móvil de confianza para acceder a los servicios públicos en línea de manera segura y conveniente.

Los ciudadanos esperan que su aplicación de identidad móvil respaldada por el gobierno admita el acceso rápido y fácil a los servicios públicos y privados en línea, en cualquier momento, a través de una autenticación sin inconvenientes que requiere un cambio mínimo en su comportamiento normal. Por supuesto, también esperan que la identidad móvil proporcionada por las autoridades públicas sea segura, siempre.

Gracias a que el acceso a los servicios públicos en línea y el proceso de completar las transacciones en línea ahora son mucho más fáciles, las soluciones de identidad móvil pueden ofrecer una conveniencia excepcional. Sin embargo, este gran cambio está acompañado por amenazas a la seguridad móvil nuevas y cada vez más numerosas. Se están propagando tipos de malware novedosos a través de una amplia gama de métodos: de tiendas de aplicaciones no oficiales, de correos electrónicos que contienen virus en sus archivos adjuntos, de aplicaciones legítimas que han sido infectadas con troyanos, y dese computadoras hasta teléfonos móviles.

Cuando se trata de proteger sus aplicaciones, los gobiernos y los proveedores oficiales de identidad nacional digital que se embarcan en esquemas de identidad nacional móvil deben resolver un rompecabezas complejo:

- Maximizar el alcance del usuario, a pesar de la fragmentación de los dispositivos móviles.
- Abordar la falta de control de los dispositivos móviles en el campo y cómo se utilizan.
- Mantener la conveniencia del usuario final con soluciones de autenticación que funcionen para todos.

Las aplicaciones de identidad móvil que contienen credenciales de identidad del usuario y claves privadas deben estar protegidas en todo momento. Esa es la razón por la cual Mobile Security Core de Gemalto ha sido diseñado para brindar la mejor seguridad de su clase para proteger la aplicación inteligente de identidad móvil (Mobile ID Smart App) de Gemalto y, más ampliamente, las billeteras de documentos de identidad digital de Gemalto contra
amenazas y ataques de malware, al tiempo que cumple con los requisitos gubernamentales. Garantiza funciones de seguridad adecuadas para todos los tipos de puntos de contacto digitales en los canales en línea. Mobile Security Core de Gemalto es desarrollado y mantenido por Gemalto, con seguridad de grado gubernamental examinada por auditorías internas y externas.

¿Cómo funciona?

Mobile ID Smart App y Mobile ID Document Wallet de Gemalto se basan en el Mobile Security Core de Gemalto. Este paquete completo de protección de aplicaciones móviles integra todas las mejores prácticas que Gemalto ha desarrollado e implementado durante muchos años en el mundo de la identidad digital y la autenticación móvil para asegurar las aplicaciones de Gemalto y garantizar la integridad de sus datos.

La lista de vulnerabilidades potenciales dentro de las aplicaciones móviles desprotegidas es extensa. Con Mobile Security Core de Gemalto en su interior, la aplicación inteligente de identidad móvil de Gemalto se asegura de que se beneficie de las últimas técnicas de protección, y ofrece a sus ciudadanos y residentes una identidad digital segura basada en dispositivos móviles.

Mobile Security Core de Gemalto

Mobile Security Core de Gemalto permite a Mobile ID Smart App y a Digital ID Document Wallet lo siguiente:

Defender
> La integridad de la aplicación móvil
> Activos sensibles

Detectar
> Entornos inseguros
> Intentos de ataque

Reaccionar
> Detener una ejecución
> Llevar a cabo acciones personalizadas, como advertir a los usuarios o enviar una alerta a un servidor de gestión de riesgos

Características de seguridad avanzadas y personalizadas

Mobile Security Core de Gemalto se basa en 4 pilares principales:

RASP *(Runtime Application Self Protection)*
Esta tecnología de seguridad está incorporada en una aplicación y es capaz de controlar la ejecución de la aplicación, detectar y prevenir ataques en tiempo real. Puede detectar entornos no seguros y también *hackers o malware* que intentan examinar las aplicaciones en tiempo de ejecución y/o manipular su comportamiento. Incluye, pero no se limita a, las siguientes tecnologías:
> Detección JB/Root > Anti-manipulación
> *Anti-Hooking* > Anti-Emulador
> Anti-Depurador

Almacenamiento seguro
Esto ofrece un área segura independiente de la plataforma para almacenar datos confidenciales de las aplicaciones, gracias a técnicas como el cifrado de múltiples capas, el anclaje al dispositivo *(device binding) y el White Box Crypto* (WBC). El objetivo del WBC es realizar una criptografía segura en entornos no seguros, en cualquier tipo de teléfono inteligente, lo que permite un nivel uniforme de seguridad en todas las plataformas y proporciona aislamiento del sistema operativo. El WBC de Gemalto se beneficia de la reconocida experiencia de Gemalto en la seguridad de las tarjetas inteligentes, como la protección contra ataques de canal lateral.

Ofuscación
Gemalto ha desarrollado su propia tecnología para ofuscar el código nativo con varias técnicas patentadas. Los principales beneficios son:
> La diversificación de los mecanismos de seguridad por cliente, evitando la replicación de un ataque de un esquema de identidad a otro.
> Impacto limitado solo al rendimiento para aplicar la ofuscación más fuerte solo en las partes críticas.
> Los gobiernos pueden usar sus herramientas de compilación estándar.

Interfaz segura
Debido a que todo está dibujado, el teclado seguro de Gemalto (GSK, por sus siglas en inglés) no depende de los servicios de teclado de la plataforma. En lugar de mantener la contraseña en la memoria, la indexa en una tabla y ofrece una visualización aleatoria de dígitos, así como una interfaz de usuario personalizable.

***Mobile Security Core* de Gemalto** protege la aplicación *Mobile ID Smart App y la billetera Digital ID Document Wallet de* Gemalto contra el malware más sofisticado y asegura uno de los activos más valiosos: la CONFIANZA de los ciudadanos.

ESPECIFICACIONES TÉCNICAS

Plataformas que admite
> iOS 10.0 y posteriores
> Android 5.0 y posteriores

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

Almacenamiento seguro
> AES
> SHA 256
> Anclaje al dispositivo (device binding)
> White Box Crypto

Ofuscación avanzada de código nativo con técnicas propietarias de Gemalto.

Reacciones personalizadas (crash o application call back)

Teclado seguro
> IU personalizable
> Cifrado punta a punta

GEMALTO.COM/LATAM

gemalto
security to be free