Gemalto Mobile Security Core

Estabelecendo uma base de confiança para permitir que a nossa aplicação móvel Smart ID e o conjunto de soluções para identidade digital detectem, reajam e defendam seus serviços de ataques de malware.

Para que serve?

A acessibilidade é fundamental para o sucesso e para a adoção dos serviços digitais. O grande volume de smartphones em todo o mundo (estima-se que haverá cerca de seis bilhões em 2020, segundo a empresa de pesquisa de mercado IHS) oferece aos governos, portanto, uma oportunidade atraente de fornecer aos cidadãos uma identidade móvel confiável para acessar serviços públicos on-line com segurança e conveniência.

Os cidadãos esperam que seu aplicativo de identidade digital, desenvolvido pelo governo, ofereça acesso rápido a serviços públicos e privados on-line, a qualquer momento, por meio de autenticação conveniente, que exige mudanças mínimas no modelo padrão existente. Evidentemente, eles também esperam que a identidade móvel fornecida pelas autoridades públicas seja sempre segura.

As soluções de identidade digital podem oferecer muita conveniência, com acesso fácil e rápido aos serviços públicos on-line, além de uma conclusão mais rápida das transações. No entanto, essa mudança no processo é acompanhada por novas e numerosas ameaças à segurança. Novos tipos de malware estão se espalhando de diversas formas: lojas de apps não oficiais, e-mails contendo vírus em seus anexos, aplicações legítimas que foram "trojanizadas" e telefones celulares.

Quando se trata de proteger suas aplicações, os governos e os provedores de identidades digitais nacionais que embarcam neste novo mundo digital precisam resolver um quebra-cabeça complexo:

- Maximizar o alcance do usuário apesar da fragmentação dos dispositivos móveis
- Abordar a falta de controle dos dispositivos móveis em campo e como eles são usados
- Manter a conveniência do usuário final com soluções de autenticação que funcionam para todos

Apps de identidade móvel que contêm credenciais com informações do usuário que devem sempre ser protegidos. É por isso que o Gemalto Mobile Security Core foi projetado: para oferecer o que há de melhor em termos de segurança e proteger o Mobile ID Smart App lançado recentemente. Além de assegurar também as carteiras digitais de documentos de identidades dos governos contra as ameaças e os ataques de malware, ao mesmo tempo em que cumpre com os regulamentos vigentes. Isso garante recursos de segurança apropriados para todos os pontos de contato digitais nos canais on-line. O Gemalto Mobile Security Core é desenvolvido e mantido pela Gemalto, com segurança de nível governamental verificada por auditorias internas e externas.

Como funciona?

A solução Mobile ID Smart App e as carteiras digitais para documentos da Gemalto são baseadas na aplicação Mobile Security Core. Esta abrangente suíte de proteção de aplicativos móveis integra todas as melhores práticas que a Gemalto desenvolveu e implementou ao longo de muitos anos em identidade digital e de autenticação móvel para proteger aplicações de identidade e garantir a integridade de seus dados.

A lista de possíveis vulnerabilidades em termos de aplicativos móveis desprotegidos é longa. Com o Mobile Security Core integrado, a solução Mobile ID Smart App garante que você se beneficie das mais recentes técnicas de proteção e oferece aos seus cidadãos e residentes uma identidade digital segura pronta para ser utilizada em dispositivos móveis.

Gemalto Mobile Security Core

O Mobile Security Core da Gemalto permite que a solução de Mobile ID Smart App e as carteiras digitais de documentos da Gemalto:

Defendam
> A integridade do aplicativo móvel
> Os ativos sensíveis

Detectem
> Ambientes inseguros
> Tentativas de ataque

Reajam
> A interrupção da execução do serviço
> A execução de ações personalizadas, tais como avisar usuários ou enviar um alerta para um servidor de gerenciamento de riscos

Recursos de segurança avançados e personalizados

O Mobile Security Core da Gemalto conta com quatro pilares principais:

RASP

Essa tecnologia de segurança é integrada no aplicativo e é capaz de controlar a execução de aplicações e detectar e impedir ataques em tempo real. Ela pode detectar ambientes inseguros e também hackers ou malware que tentam investigar as aplicações durante sua execução e/ou adulterar seu comportamento. Inclui às seguintes tecnologias, entre outras:

> Detecção de Jailbreak/root > Antiviolação

> Anti-Hooking > Antiemulador

> Antidepurador

Armazenamento seguro

Ele oferece uma área segura independente da plataforma para armazenar dados confidenciais das aplicações graças a técnicas como a criptografia multicamadas, vinculação de dispositivos e White Box Crypto (WBC). O objetivo da WBC é executar a criptografia segura em ambientes inseguros, em qualquer tipo de smartphone, permitindo um nível uniforme de segurança em todas as plataformas e oferecendo isolamento do sistema operacional. A WBC da Gemalto se beneficia da conhecida experiência da Gemalto em segurança para cartões inteligentes, como a proteção contra ataques de canal lateral.

Ofuscação

A Gemalto desenvolveu sua própria tecnologia para ofuscar o código nativo com várias técnicas patenteadas. Os principais benefícios são:

> Diversificação dos mecanismos de segurança por cliente, evitando a replicação de um ataque de um esquema de identidade para outro.
> Impacto limitado apenas ao desempenho, para aplicar a ofuscação mais forte somente em partes críticas.
> Os governos podem usar suas ferramentas de compilação padrão.

Interface Segura

Como tudo é desenhado sob medida, o Gemalto Secure Keypad (GSK) não depende dos serviços de teclado da plataforma. Em vez de manter a senha salva, ele a indexa em uma tabela e oferece uma exibição aleatória de dígitos, bem como uma interface de usuário personalizável.

O **Mobile Security Core da Gemalto** protege as soluções de Mobile ID Smart App e as carteiras digitais de documentos dos governos de ataques de malware mais sofisticados, garantindo, assim, um dos ativos mais valiosos: **a CONFIANÇA dos cidadãos.**

ESPECIFICAÇÕES TÉCNICAS

Plataformas suportadas
> iOS 10.0 e superior
> Android 5.0 e superior

Proteção RASP
> Detecção de jailbreak/root
> Detecção de ferramentas de ocultação de jailbreak/root
> Anti-Hooking
> Antidepuração
> Antiviolação estática
> Antiemulador
> Antiadulteração dinâmica

Armazenamento seguro
> AES
> SHA 256
> Vinculação do dispositivo
> White Box Crypto

Ofuscação Avançada de código nativo com técnicas da Gemalto

Reações personalizadas (chamada de retorno de aplicação ou falha)

Teclado Seguro
> Interface do usuário personalizável
> Criptografia de ponta a ponta

THALES
→ GEMALTO.COM.BR

gemalto
a Thales company