



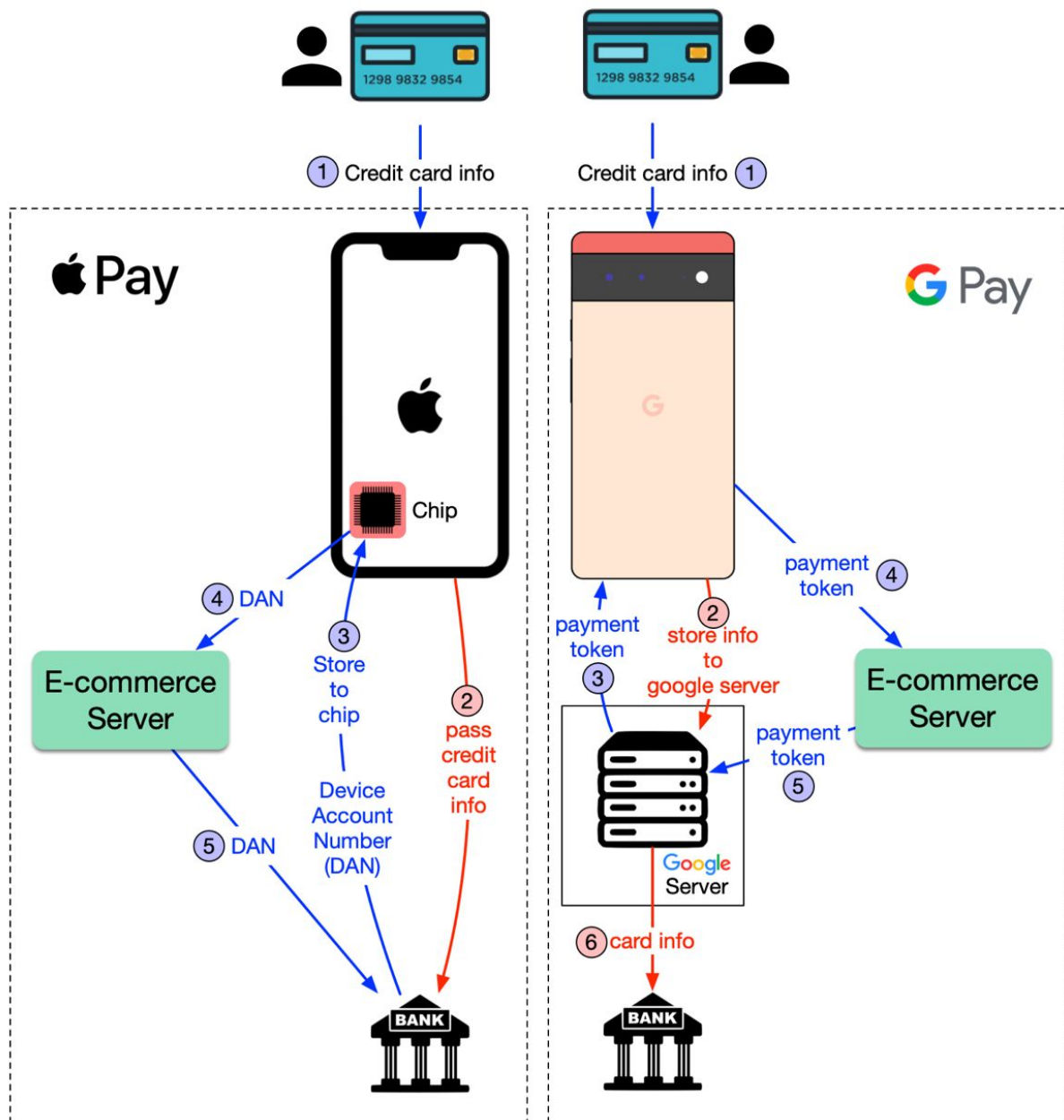
Universidad de Buenos Aires
Facultad de Ciencias Económicas



Apple Pay y Google Pay - Funcionamiento



Material de Estudio



Objetivo del mecanismo de seguridad

Tanto **Apple Pay** como **Google Pay** están diseñados para **evitar que el número real de la tarjeta de crédito circule por la red** durante una transacción.

En su lugar, utilizan **tokenización**, un principio clave en los **Sistemas de Información de pagos**.

Concepto central: Tokenización (Tokenization)

- **Tokenización (Tokenization):** proceso mediante el cual el número real de la tarjeta se reemplaza por un **token** (identificador sustituto).
 - El token **no tiene valor fuera de ese contexto** y no puede reutilizarse.
 - Reduce drásticamente el riesgo de fraude, filtraciones de datos y responsabilidades legales.
-

Flujo de seguridad en Apple Pay

1. Registro de la tarjeta

El usuario ingresa la información de su tarjeta de crédito en el dispositivo.

2. Envío de la información al banco

Los datos reales de la tarjeta se envían al banco emisor para validación.

3. Generación del DAN

El banco genera un **DAN – Device Account Number (Número de Cuenta del Dispositivo)**:

- Es un número sustituto de la tarjeta real.
- Está asociado **a ese dispositivo específico**.

4. Almacenamiento seguro

El DAN se guarda en un **chip seguro del dispositivo** (*Secure Element*):

- El número real de la tarjeta **no se almacena** en el teléfono.
- Apple no puede acceder al número real de la tarjeta.

5. Pago en un comercio

Cuando se realiza un pago:

- El dispositivo envía el **DAN** al servidor del comercio electrónico (*E-commerce Server*).
- El comercio nunca recibe el número real de la tarjeta.

6. Autorización bancaria

- El banco recibe el DAN.
- Lo traduce internamente al número real.
- Autoriza o rechaza la operación.

Clave administrativa:

Apple Pay **descentraliza el riesgo**, apoyándose en hardware seguro y minimizando la exposición de datos sensibles.

Flujo de seguridad en Google Pay

1. Registro de la tarjeta

El usuario ingresa la información de su tarjeta en el dispositivo Android.

2. Almacenamiento en servidores de Google

La información de la tarjeta se guarda de forma segura en los **servidores de Google**.

3. Generación del token de pago

Google genera un **Payment Token (Token de Pago)**:

- Representa a la tarjeta real.
- Se utiliza exclusivamente para transacciones.

4. Pago en el comercio

El dispositivo envía el **token de pago** al servidor del comercio electrónico.

5. Validación del token

El comercio reenvía el token a los servidores de Google para validación.

6. Autorización bancaria

- Google envía la información necesaria al banco.
- El banco valida y autoriza la transacción.

Clave administrativa:

Google Pay **centraliza más información en la nube**, apoyándose en su infraestructura de servidores para la seguridad.

Diferencias clave desde la perspectiva de Sistemas de Información

Apple Pay

- Uso intensivo de **hardware seguro**.
- Datos sensibles almacenados en el dispositivo.
- Menor dependencia de servidores externos para la custodia de la tarjeta.
- Menor superficie de ataque en la nube.

Google Pay

- Uso intensivo de **infraestructura en la nube**.
 - Mayor dependencia de servidores centrales.
 - Escalabilidad y control centralizado.
 - Más puntos de control, pero también más puntos críticos.
-

Elementos tecnológicos clave involucrados

- **DAN – Device Account Number (Número de Cuenta del Dispositivo)**
 - **Payment Token – Token de Pago**
 - **Secure Element – Elemento Seguro (chip físico)**
 - **E-commerce Server – Servidor de Comercio Electrónico**
 - **Bank / Issuer Bank – Banco Emisor**
-

Implicancias para la administración

Gestión del riesgo

- La tokenización reduce la exposición a fraudes y brechas de datos.
- Disminuye el impacto económico y reputacional de incidentes de seguridad.

Cumplimiento normativo

- Facilita el cumplimiento de normativas de protección de datos y estándares de seguridad (por ejemplo, PCI DSS).
- Menor manejo directo de datos sensibles por parte del comercio.

Decisiones de arquitectura

- Apple Pay prioriza **seguridad en el dispositivo**.
 - Google Pay prioriza **seguridad en la nube**.
 - La elección impacta en costos, escalabilidad, soporte y dependencia tecnológica.
-

Idea central a retener

Ni Apple Pay ni Google Pay transmiten el número real de la tarjeta durante una compra.

Ambos sistemas se basan en **tokenización**, pero con **arquitecturas distintas**:

- Apple Pay: seguridad apoyada en hardware.
- Google Pay: seguridad apoyada en infraestructura de servidores.

Desde la administración y los sistemas de información, comprender estas diferencias es esencial para **evaluar riesgos, responsabilidades y decisiones tecnológicas en medios de pago digitales.**

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos)**, los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.

La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.

Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.

Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.

Queda expresamente excluido cualquier uso con fines comerciales.