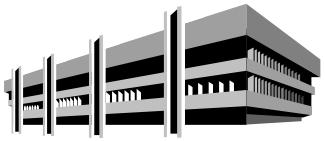
Certificación Digital y Sistemas de Pago

Temario

- La seguridad en Internet y el Sistema de Pagos
- Los Certificados Digitales
- Una estrategia país viable

El sistema de pagos de Costa Rica



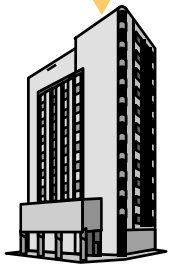
Cliente Origen

Relación privada

Clientes Destino

Medios:
Sitios Web
Sucursales
Otros

- Bancos
- Financieras
- Mutuales
- Cooperativas
- Instituciones Públicas



Entidad Origen

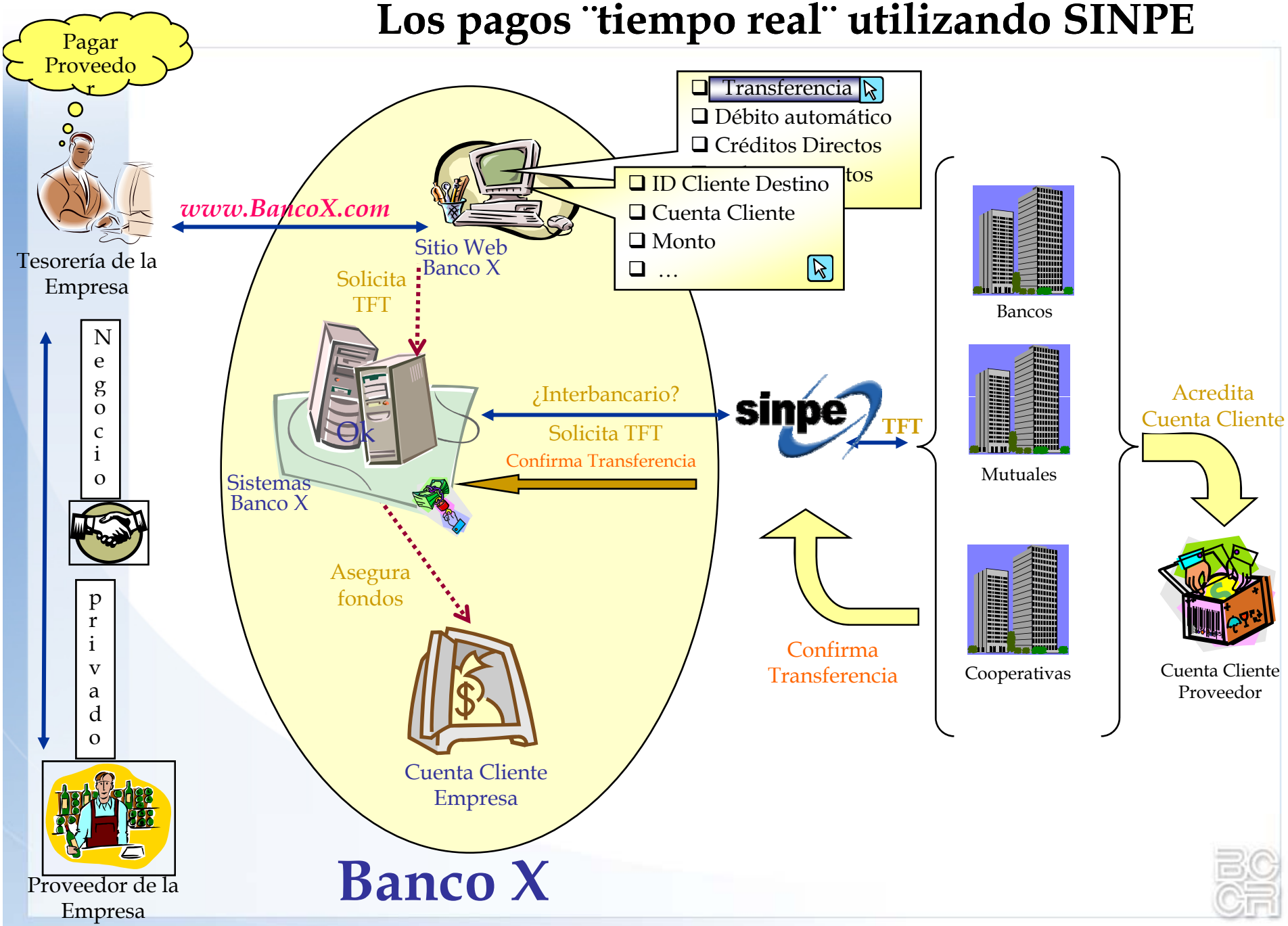
sinpe

Entidades Destino

- Bancos
- Mutuales
- Cooperativas

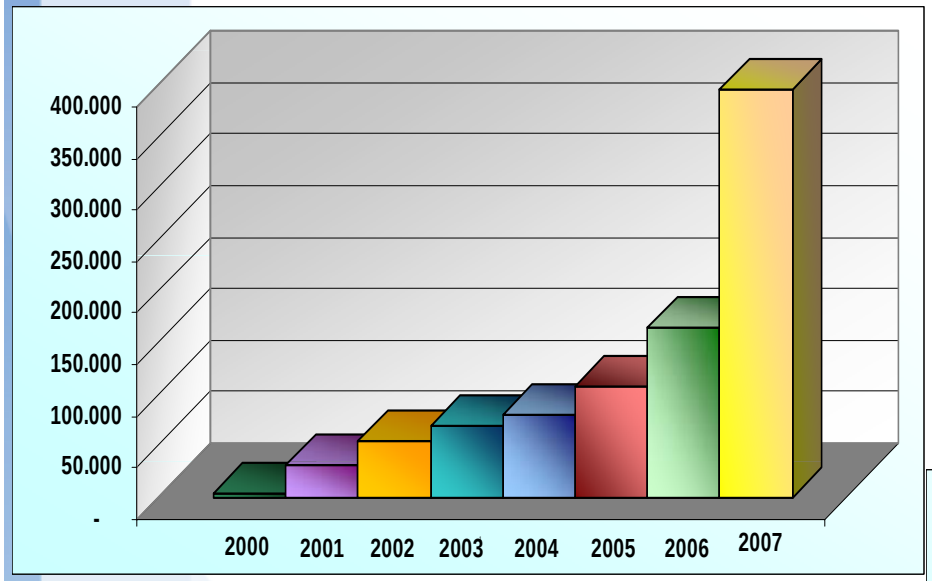
Servicios:
- Transferencias en Tiempo Real (Pago)
- Débito en Tiempo Real (Cobro)
- Créditos Directos (Pago)
- Débito Directo (Cobro)
- Cámara de Cheques
- Servicios para Tesorería (CAN)
- Compra y Venta de Divisas
- Otros (más de 20)

Los pagos ¨tiempo real¨ utilizando SINPE

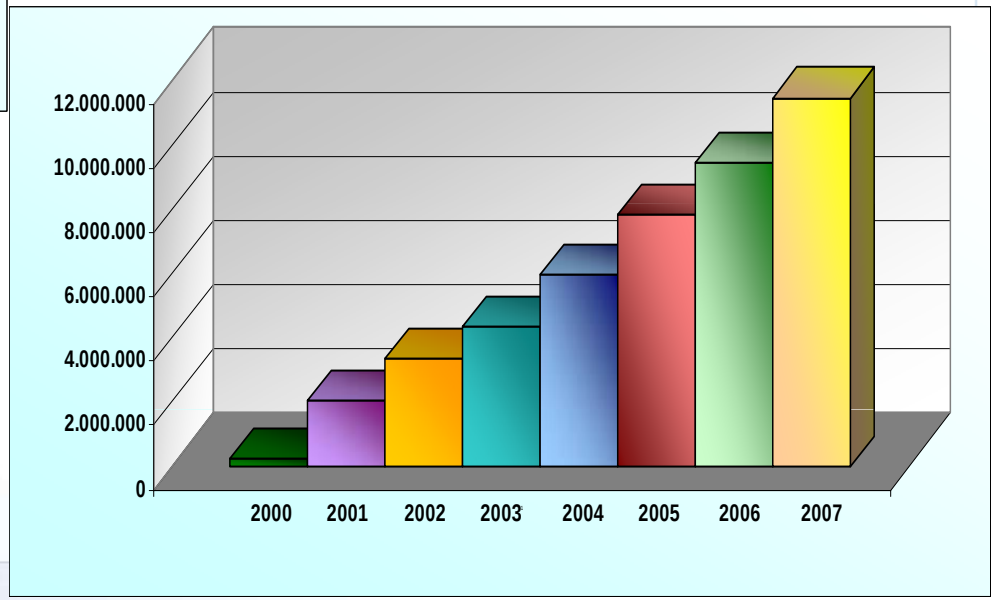


Transferencias de Fondos a Terceros
Período: 2000-2007

Cantidad de Transacciones Enviadas



Monto de Transacciones Liquidadas (en millones de colones y colones equivalentes)



Débito en Tiempo Real (DTR) en aduanas (Gobierno Digital)

Agente Aduanal
Importador
Exportador

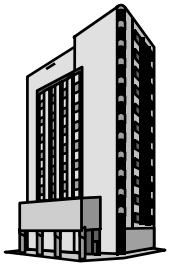
Solicitud
Confirmación

TICA

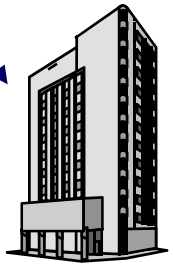
Sistema Aduanero
de Costa Rica

Orden de Débito
Depósito:
- Cuenta: XXX
- Monto: YYY

sinpe



Entidad financiera
del cliente A



Entidad financiera
del cliente B

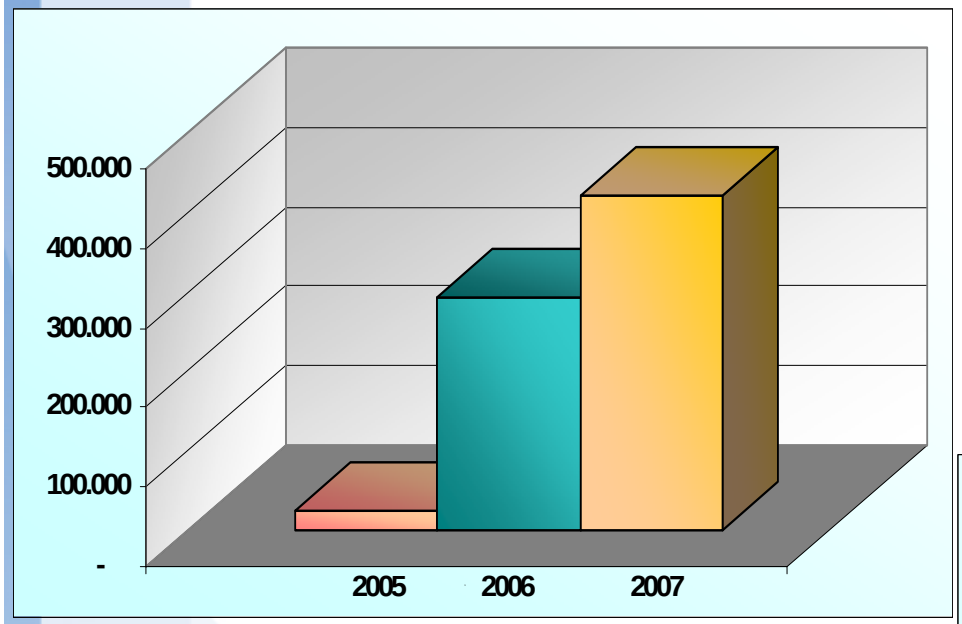
Tesorería Nacional
Contabilidad Nacional

Aduanas

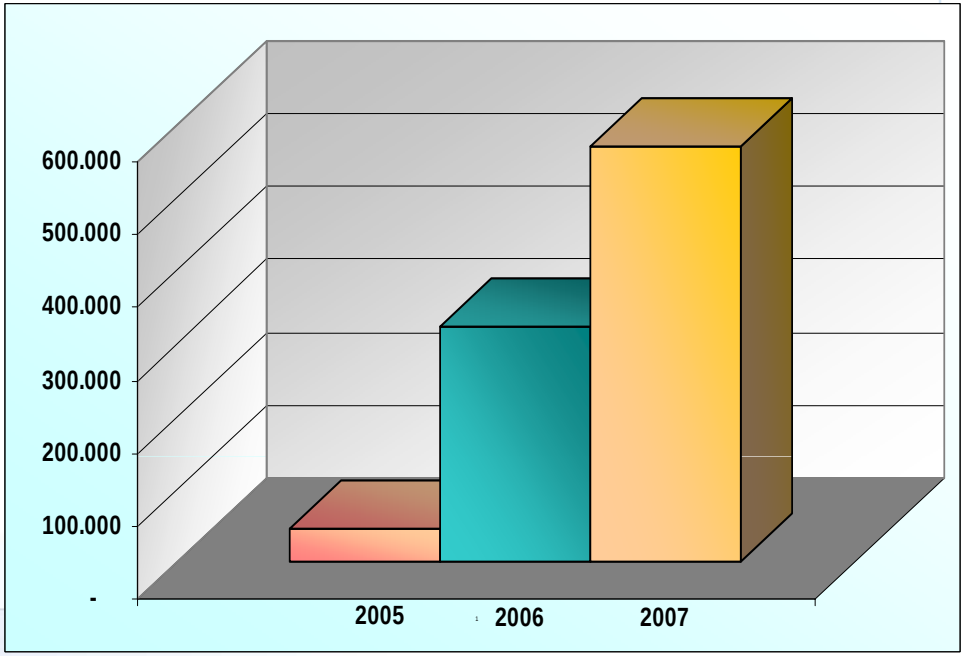
- Caldera
- Santamaria
- LIMON
- Paso Canoas
- Peñas Blancas
- Otras

Débitos en Tiempo Real
Período: 2005-2007

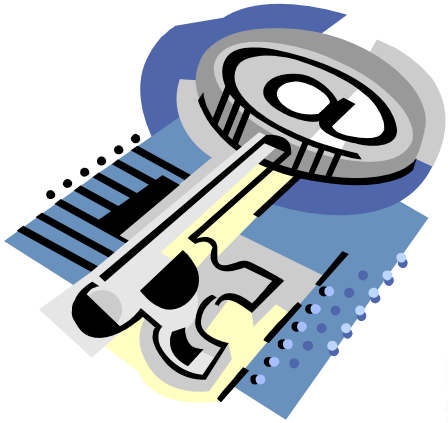
Cantidad de Transacciones Enviadas



Monto de Transacciones Liquidadas (en millones de colones y colones equivalentes)



Modelo Conceptual



Infraestructura de llave Pública (PKI)

Llaves relacionadas matemáticamente, que permiten la comunicación segura entre usuarios sin compartir llaves secretas previamente.

La Llave Privada debe mantenerse secreta, mientras que la Llave Pública puede ser distribuida.

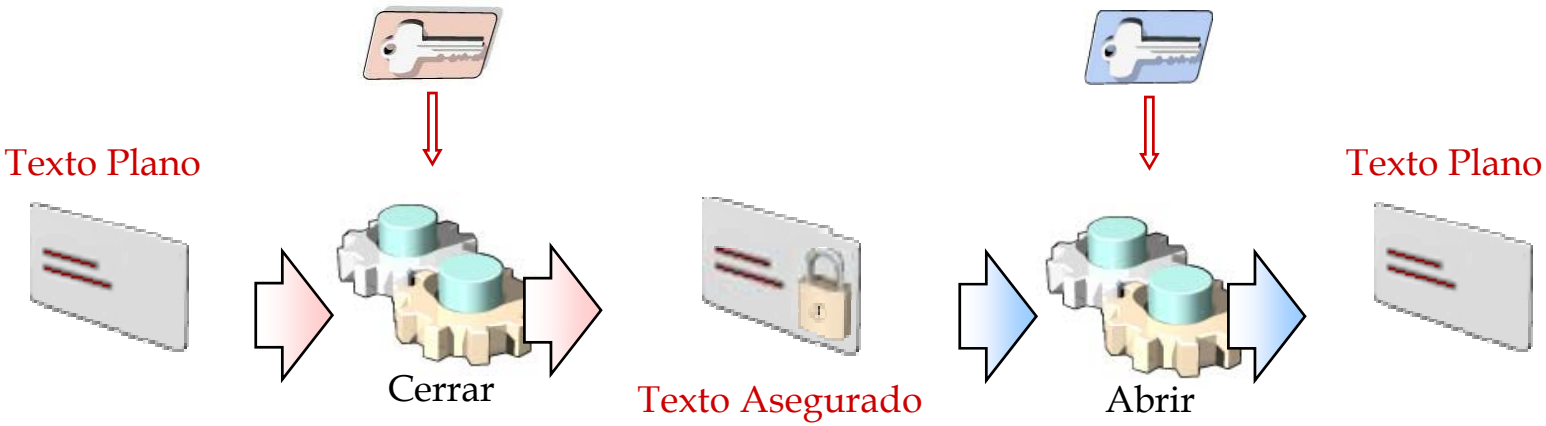
Llave Pública

Llave Privada

Es *computacionalmente* imposible deducir la Llave Privada de un par de llaves, aún cuando se posea la Llave Pública correspondiente (utilizando una longitud de llave adecuada)

Llave Pública y Privada

Puede decirse que si una de estas llaves se utiliza para "*cerrar un candado*", solamente la llave correspondiente puede ser usada para abrirlo.



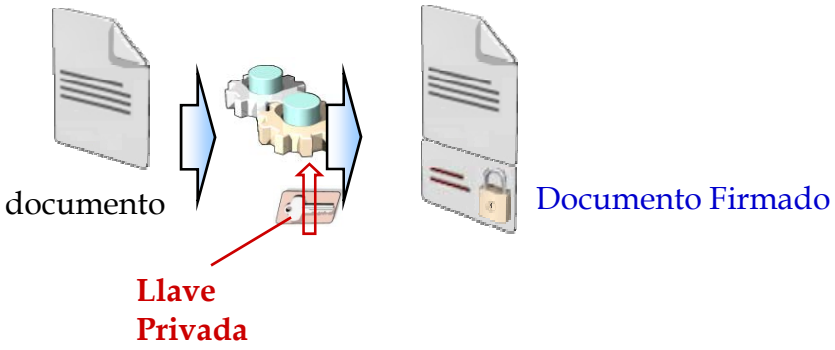
Tanto la Llave Privada como la Llave Pública pueden ser utilizadas para asegurar información.

Firma Digital

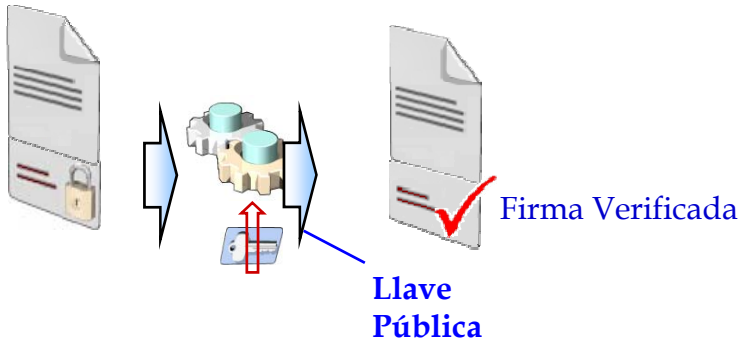
Firma Digital

En la Firma Digital se pueden identificar dos procesos básicos:

Proceso de Firma



Proceso de Verificación



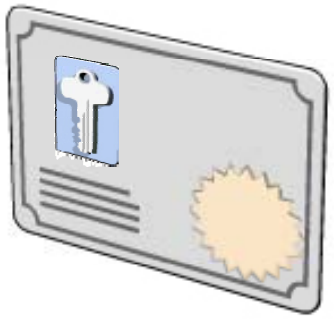
La Firma Digital garantiza la integridad y autenticidad de los documentos digitales.

Certificado Digital

El Certificado Digital es un documento electrónico que relaciona una identidad con una Llave Pública.

Sus componentes principales son:

- Una Llave Pública
- Información del dueño del certificado
- Información del emisor de ese certificado
- Periodo de validez
- Un identificador único
- La Firma Digital del emisor



Smartcards - USB Tokens

El Certificado y la Llave Privada pueden ser almacenados en tarjetas inteligentes seguras

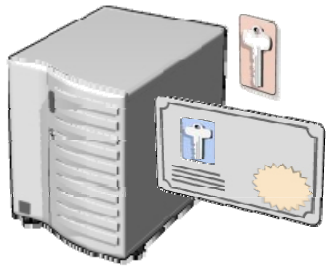
También se utilizan Tokens USB para proteger la Llave Privada y el Certificado de un titular

- Realiza las operaciones criptográficas internamente
- Las Llaves Privadas nunca son expuestas
- Uso de un PIN o clave para identificar al titular

Tokens Biométricos

- Todas las anteriores
- Uso de la Huella Digital para identificar al titular

Certificador
(Autoridad Certificadora)

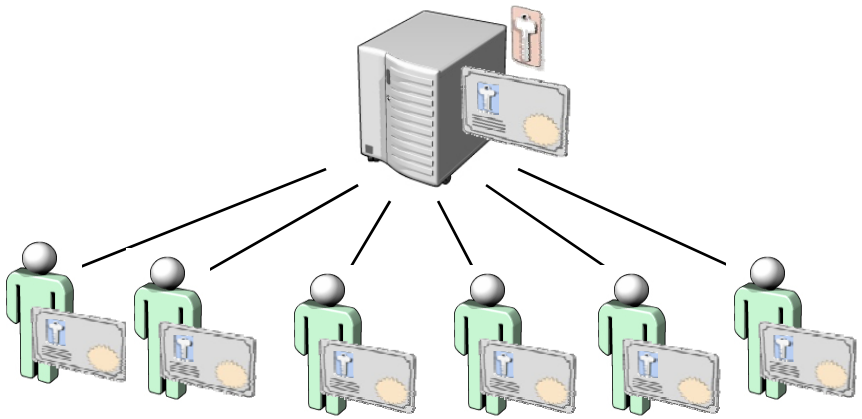


Autoridad Certificadora

Una Autoridad Certificadora es el tercero de confianza que emite Certificados Digitales

La validez de un Certificado Digital dependerá de la confianza que se tenga en el emisor del mismo

Autoridad Certificadora

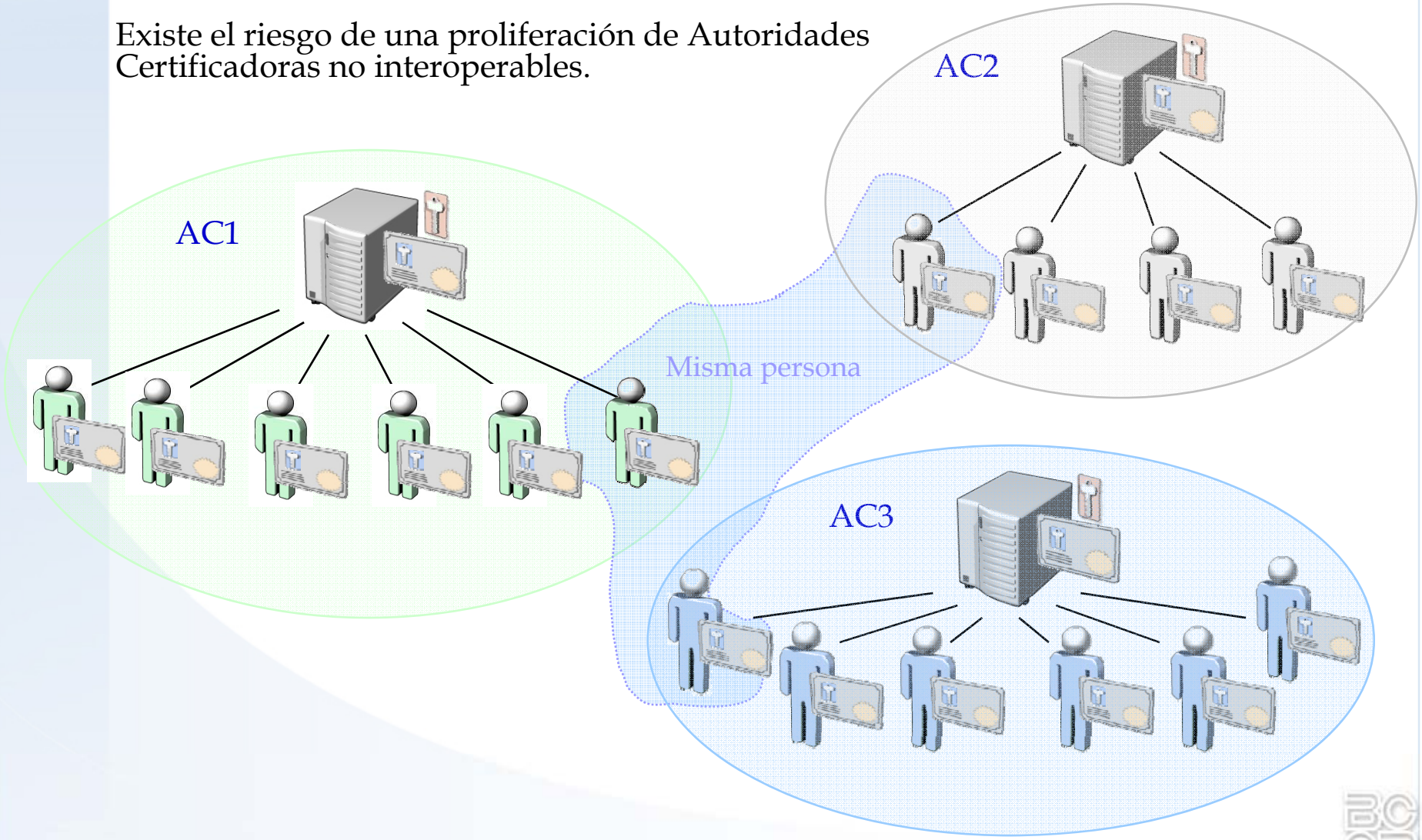


Un usuario que confía en una AC puede verificar que una Llave Pública pertenece a quien se identifica en un Certificado Digital.

Riesgo Identificado

La leyes sobre firma digitales permite la existencia de múltiples ACs.

Existe el riesgo de una proliferación de Autoridades Certificadoras no interoperables.



Hallazgos en países visitados

- Diversidad de modelos
- Dispares niveles de desarrollo
- En la mayoría no existe interoperabilidad de certificados
- Altos costos para el usuario cuando existen modelos privados
- En varios países el estado impulsa esta tecnología (básicamente para declaración de impuestos)
- Infraestructuras robustas pero aún muy bajos niveles de penetración (menores al 0.5%)

Metas para Costa Rica

- Certificados Interoperables (idénticas políticas entre emisores)
  - Creación de una raíz nacional
- Reducción de barreras de entrada:
  - Culturales (seleccionar adecuadamente la población de inicio)
  - Bajos Costos (máxima reutilización de infraestructuras existentes)
- Sostenible en el tiempo, preferiblemente sin inversión pública
- Orientado a satisfacer al usuario final
- Robusto (cumplimiento de normas internacionales ISO-21188 e ISO-27001)

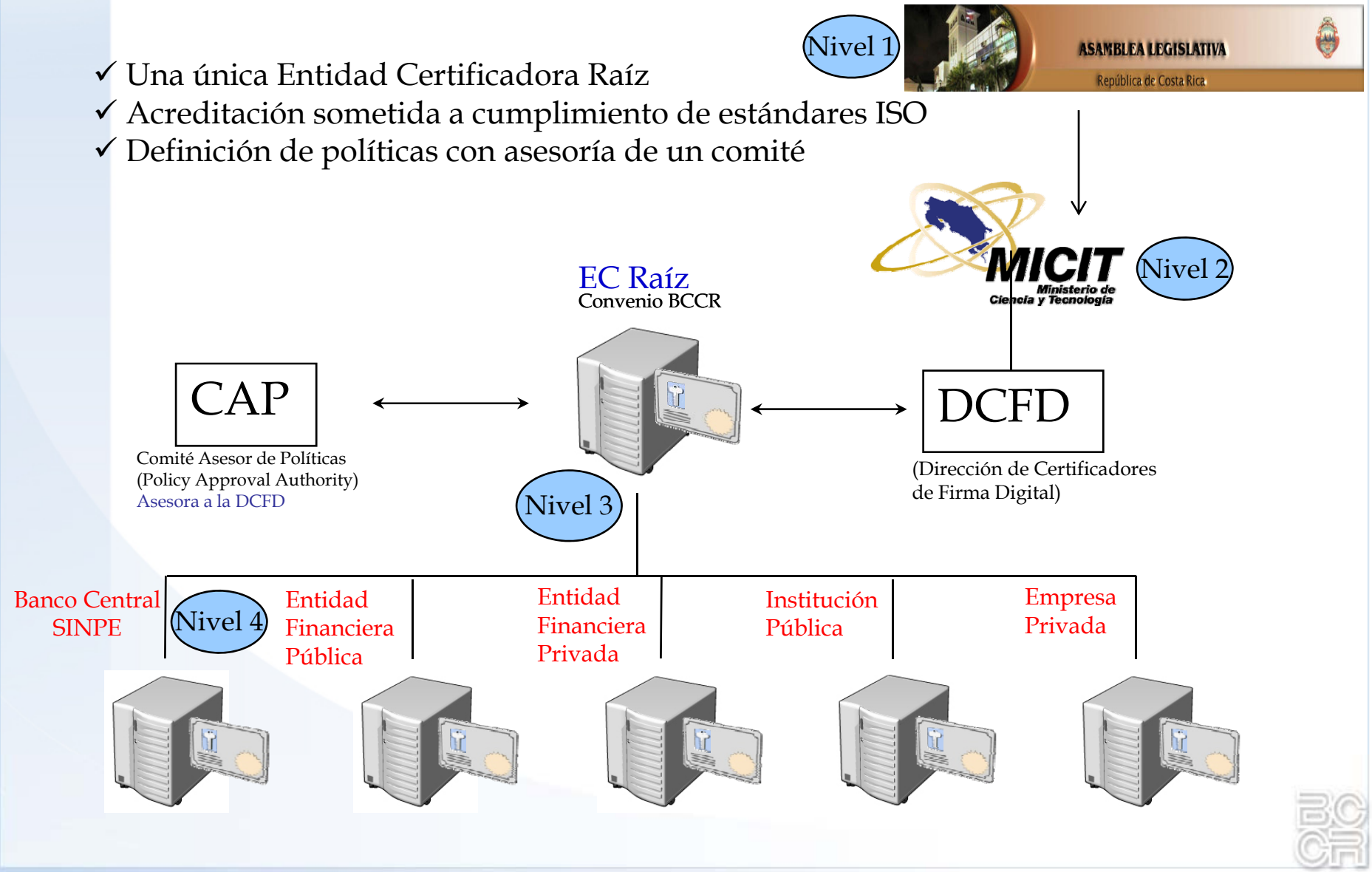
Donde están los costos?

Puesta en marcha del Sistema Nacional de Certificación Digital

- Infraestructura para la Emisión de certificados digitales
  - Autoridad Raíz
  - Autoridades Certificadoras
- Infraestructura para la Distribución de certificados digitales
  - Autoridades de Registro
- Procesos de Emisión y distribución de certificados
- Dispositivo contenedor del certificado (Smartcards o Token)
- Gestión del Sistema

Costa Rica – Actores del Modelo

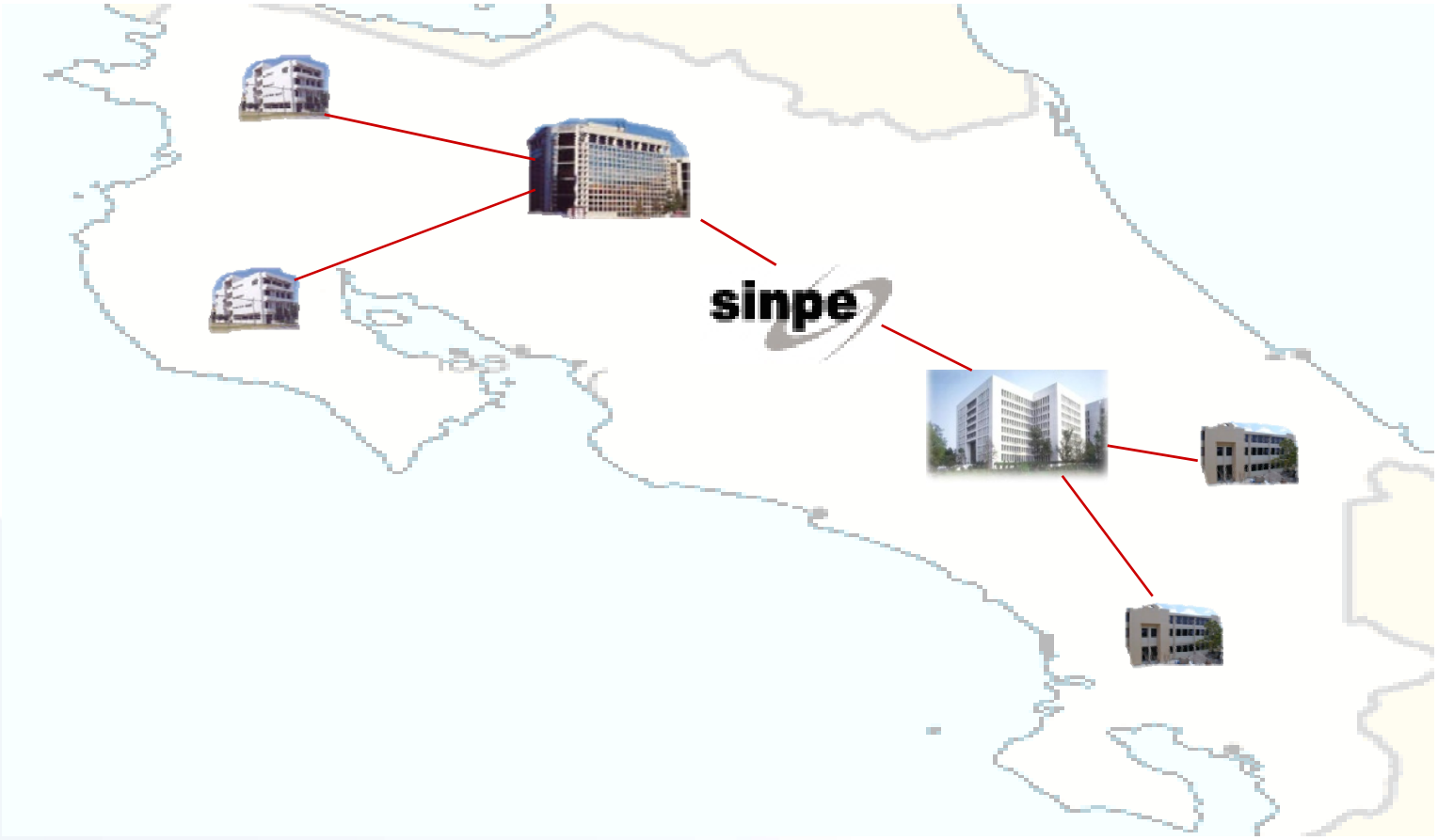
- ✓ Una única Entidad Certificadora Raíz
- ✓ Acreditación sometida a cumplimiento de estándares ISO
- ✓ Definición de políticas con asesoría de un comité



Servicio de Certificación Digital del SINPE

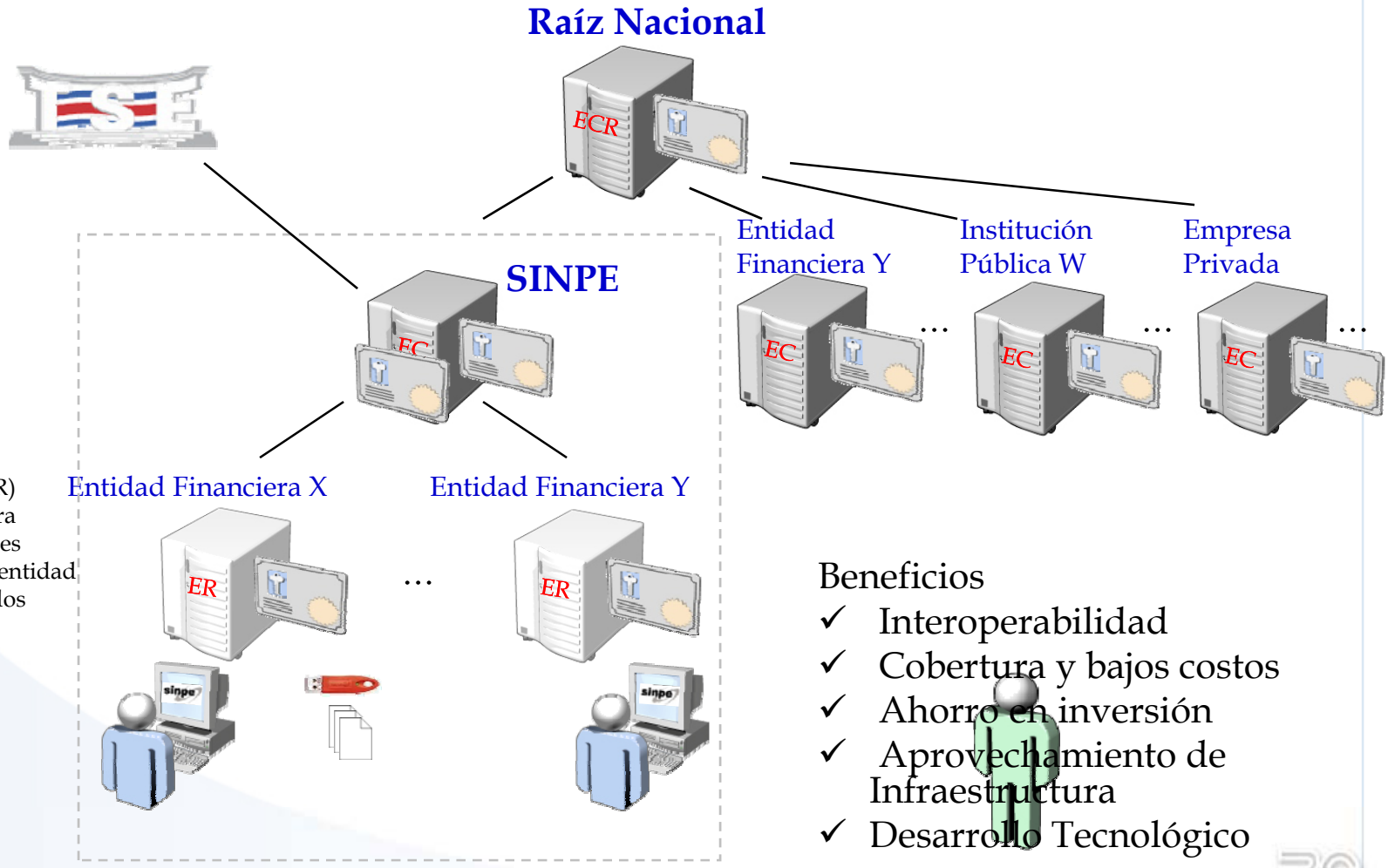
Fortalezas del Sistema Financiero

- Confianza del público en general
- Operadores del Sistema de Pagos
- Infraestructura existente
- Capacidad de registro y distribución (más de 1000 Sucursales)
- Especialistas en el "Cuide a su cliente"
- Tienen un problema que resolver



Modelo de Operación

Las Entidades Financieras funcionan como Entidades de Registro en forma voluntaria

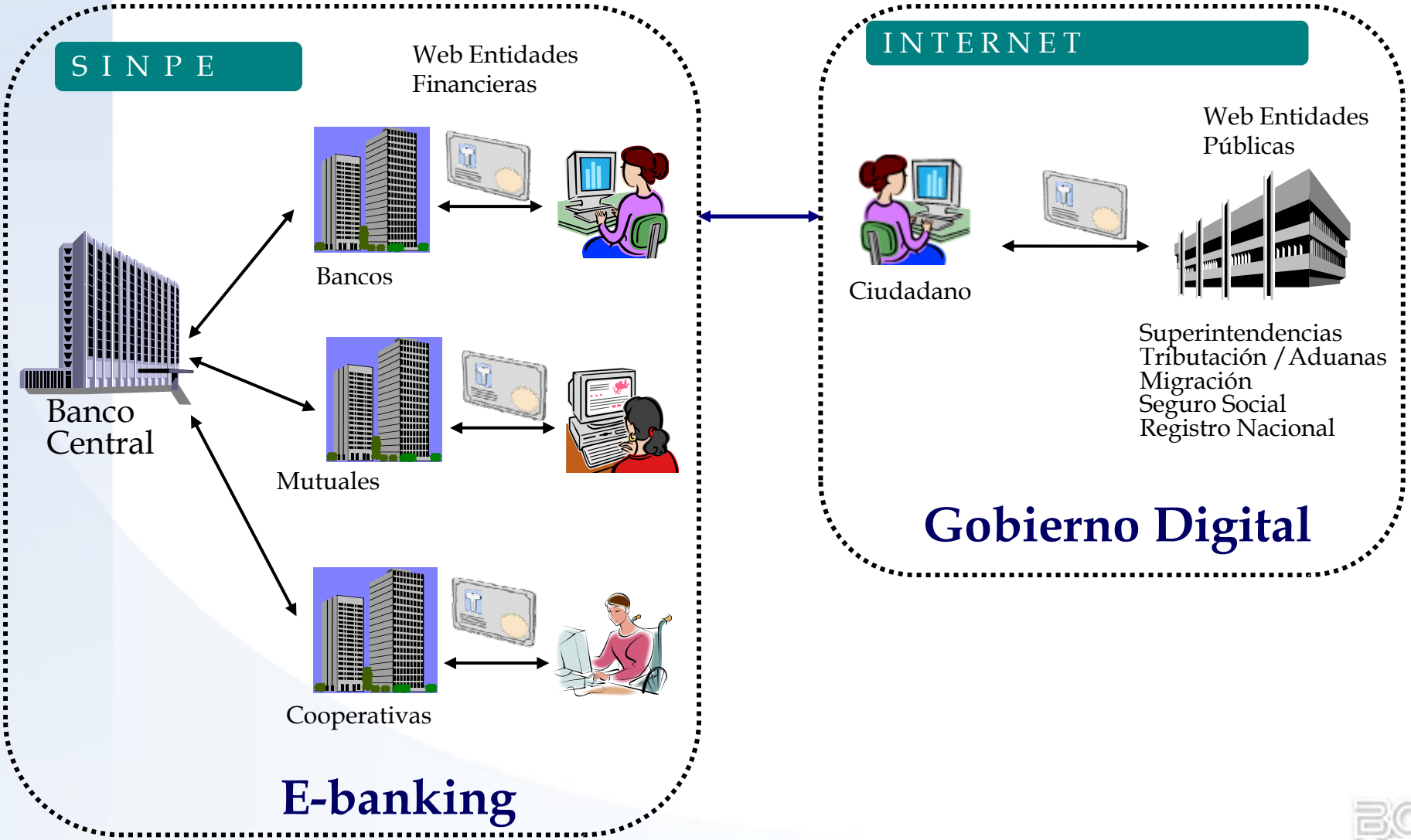


Entidad de Registro (ER)
- ✓ Provee Infraestructura
- ✓ Administra Solicitudes
- ✓ Comprobación de Identidad
- ✓ Entrega de Certificados

Beneficios
- ✓ Interoperabilidad
- ✓ Cobertura y bajos costos
- ✓ Ahorro en inversión
- ✓ Aprovechamiento de Infraestructura
- ✓ Desarrollo Tecnológico

E-banking y Gobierno Digital

E-banking y Gobierno Digital



Muchas Gracias