Biometría, Sistemas de Identificación y Control de Identidad Casos de Negocio

Marco Antonio Zúñiga
marco@maz.cl – www.maz.cl

Diciembre 2019

NOTA

- Se incluye en el anexo de este documento mucha información técnica adicional a la que realmente se revisará en este curso, dado que el foco es análisis de tecnologías biométricas y verificación de identidad desde un punto de vista del NEGOCIO.

Qué es la biometría

- La "Biometría Informática" es la aplicación de técnicas biométricas(*) a la autentificación e identificación automática de personas en sistemas de seguridad informática. Las técnicas biométricas se basan en medir al usuario directa o indirectamente para reconocerlo automáticamente aplicando técnicas estadísticas y de Inteligencia Artificial (lógica borrosa, redes neuronales, etc).

- (*) Biometría: el concepto tradicional de biometría se refiere a la aplicación de las técnicas matemáticas y estadísticas a las ciencias de los seres vivos i.e. medicina, biología, etc.

- Fuente: Agrupación de Biometría Informática Española

Qué resuelve la biometría ...

- La tercera componente de los mecanismos de autenticación ...
  - Algo que sé
  - Algo que tengo
  - **Algo que soy**

La Biometría no resuelve todo
(AB: Autenticación Biométrica)

- la AB por sí sola no puede resolver todas las necesidades de autentificación y seguridad, sino que hemos de considerarla una herramienta más dentro de nuestro repertorio.
- El ejemplo más claro es la firma digital o la encriptación dentro de una arquitectura de clave pública (PKI). Un sistema de AB puede ser complemento perfecto para la contraseña de una clave privada dentro de una PKI, pero sin el resto de elementos que forman la PKI, la AB no podría cumplir ninguno de los objetivos de irrefutabilidad, autentificación e integridad.
- Por tanto, la AB es una herramienta más en todo sistema de seguridad informática y su uso ideal es como complemento de otros sistemas de autentificación o criptografía.

- Cita de Manuel A. Delgado Tenorio

Tipos de Biometría

- Biometría **Estática**: mide la **anatomía** del usuario.
  - Huellas Digitales.
  - Geometría de la mano.
  - Termografía.
  - Análisis del iris.
  - Análisis de retina.
  - Venas del dorso de la mano.
  - Reconocimiento Facial.
- Biometría **Dinámica**: mide el **comportamiento** del usuario.
  - Patrón de Voz
  - Firma manuscrita
  - Dinámica de tecleo
  - Cadencia del paso
  - Análisis gestual

Ambitos de la Identificación

Tipos de Biometría

- Biometría Estática: mide la anatomía del usuario.
  - Huellas Digitales.
  - Geometría de la mano.
  - Termografía.
  - Análisis del iris.
  - Análisis de retina.
  - Venas del dorso de la mano.
  - Reconocimiento Facial.
- Biometría Dinámica: mide el comportamiento del usuario.
  - Patrón de Voz.
  - Firma manuscrita.
  - Dinámica de tecleo.
  - Cadencia del paso.
  - Análisis gestual.

Rasgos distintivos

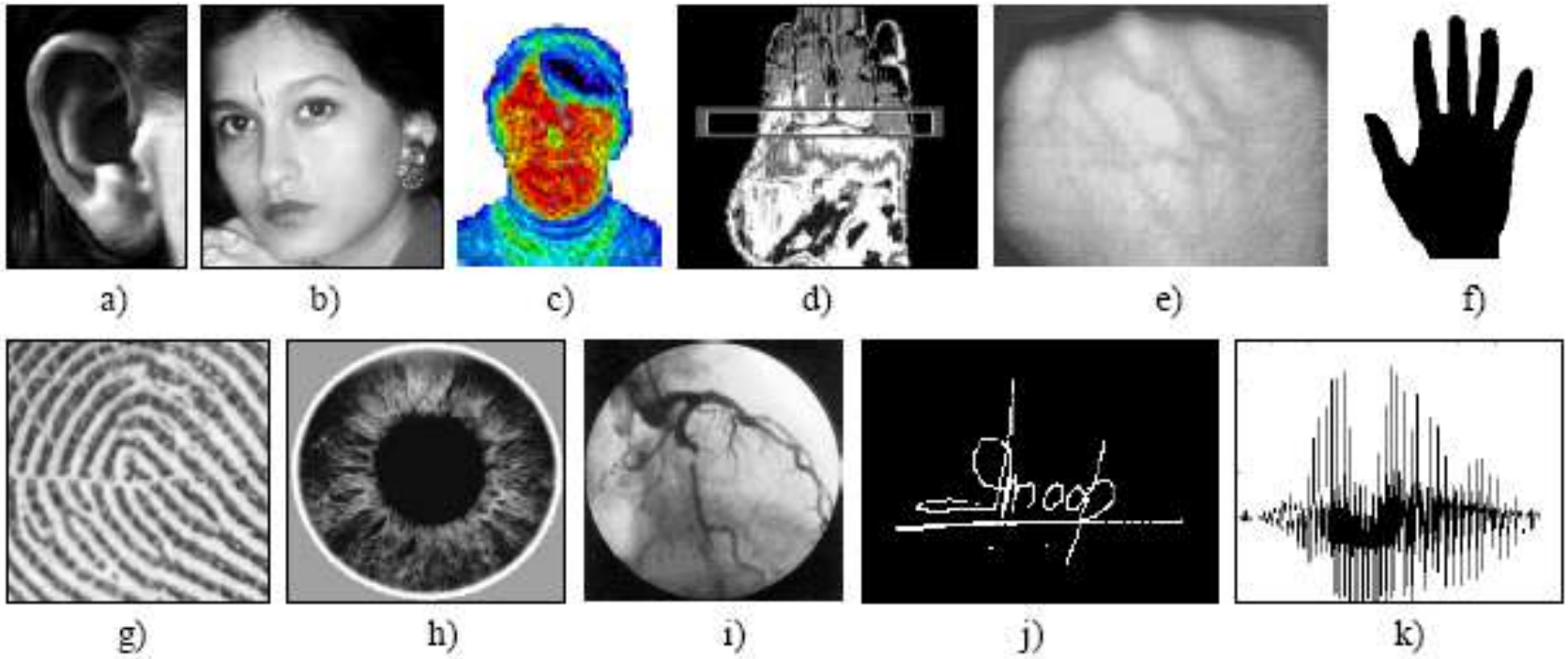


Figure 1.2. Some of the biometrics are shown: a) ear, b) face, c) facial thermogram, d) hand thermogram, e) hand vein, f) hand geometry, g) fingerprint, h) iris, i) retina, j) signature, and k) voice.

Fuente:
D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition
Springer, New York, 2003

El desafío de la biometría

- Lo ideal para un sistema de biometría es centrarse en aquellos rasgos que, además de ser distintos en cada persona, no sufren variaciones a lo largo del tiempo por causas como el proceso natural de envejecimiento o los cambios en la masa corporal

- Cita de Manuel A. Delgado Tenorio

Cómo se implementa

- Mediante algún mecanismo de medición del Rango Distintivo
- Modelo de Operación:
  - Se define un “patrón” del individuo durante el proceso de “enrolamiento”
  - Las siguientes mediciones son relativas al “patrón”
  - Los patrones pueden ser dinámicos o estáticos
- Alternativas de Identificación:
  - 1:1: Verificación de Identidad
  - 1:N: Identificación sobre un Universo predeterminado

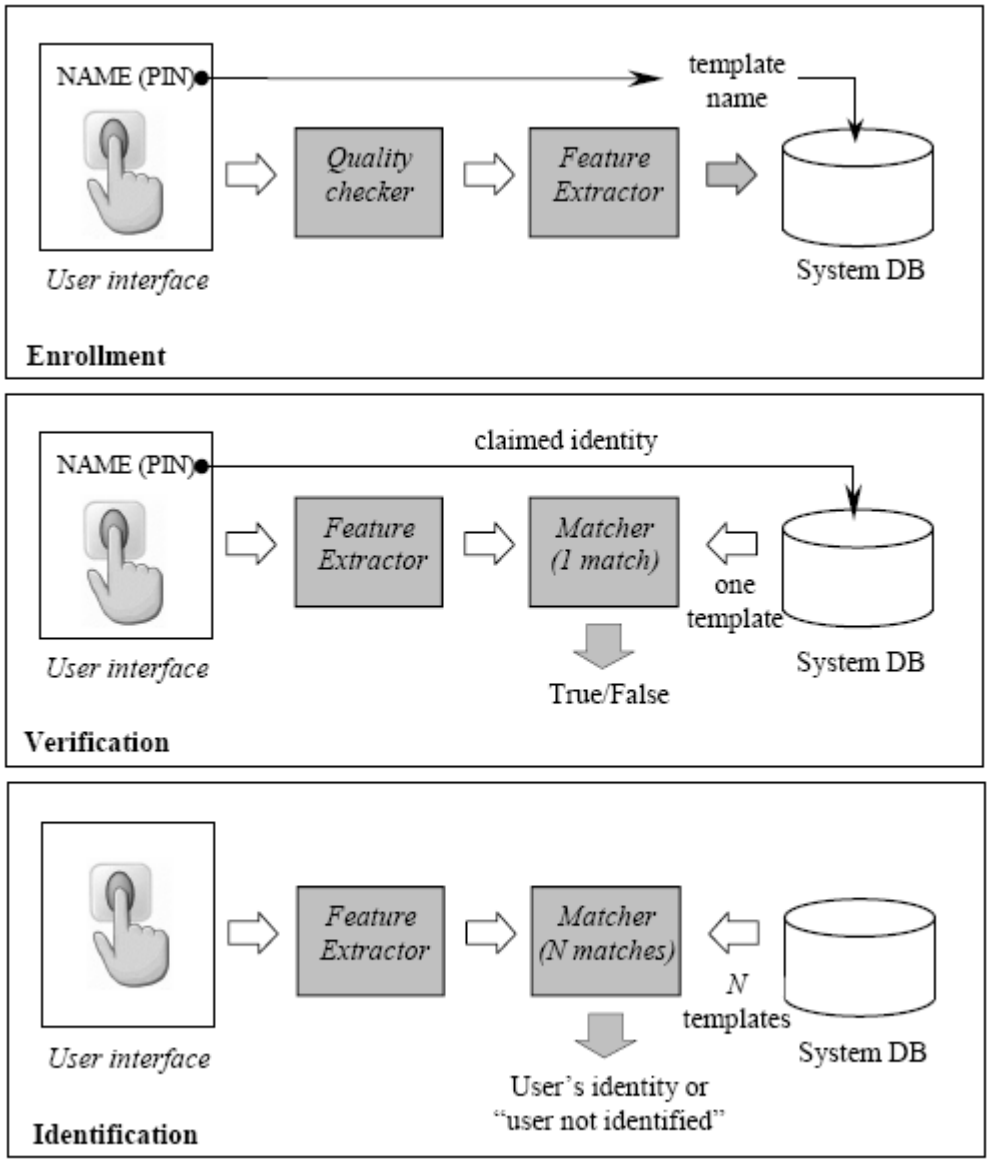


Figure 1.1. Block diagrams of enrollment, verification, and identification tasks.

Modelos de Enrolamiento, Verificación e Identificación (con Huella Digital)

(Aplicable a cualquier medida biométrica)

Fuente:

D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar
Handbook of Fingerprint Recognition
Springer, New York, 2003

Problema: Las Búsquedas

- El Problema :
  - La biometría no genera medidas “exactas”, por lo cual sólo se puede definir funciones “Distancia” (qué tan cerca está un punto de otro)
    - El error aceptado para definir dos puntos como “cercanos” o “iguales” se define como “Umbral”
  - Por tanto, no se puede definir una relación de Orden
    - No se permiten búsquedas “binarias” o por “indexación”
  - La única forma actual de “identificar” es por búsqueda secuencial
  - Es posible generar una taxonomía mediante “clusters” para acelerar las búsquedas
    - Ej: Peritos Dactilógraficos con huellas latentes

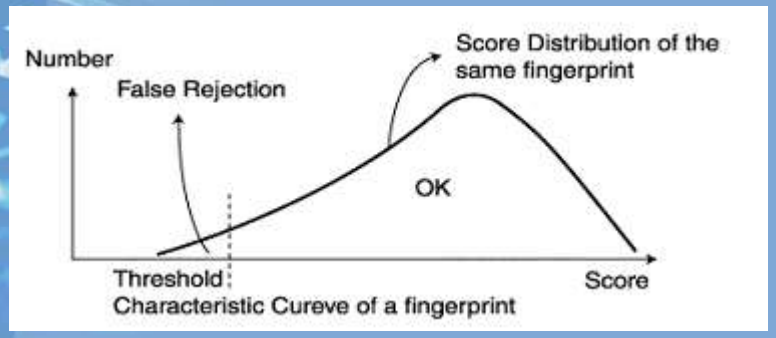
Parámetros a considerar en el diseño

- Tasas
  - Falsas aceptaciones
  - Falsos rechazos
  - Umbrales de aceptación
- Usos
  - Ambiente
  - Tipos de usuarios
  - Contexto de aplicación
- Factor crítico
  - Arquitectura de integración a sistemas y procesos
- Recomendación de puesta en marcha:
  - Iniciar con tolerancias mayores, hasta capacitar usuarios
  - Disminuir la tolerancia según la población objetivo

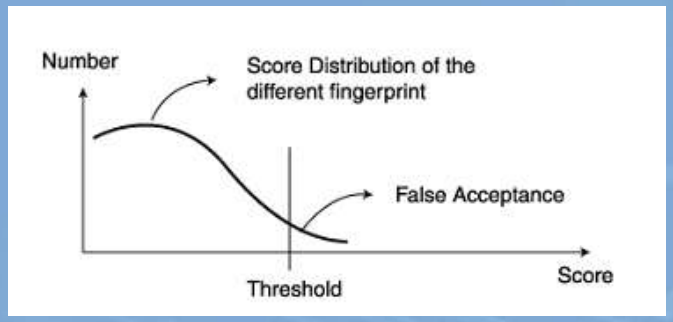
Curvas de Falsa Aceptación y Falso Rechazo

$$FAR = \frac{\text{total number of falsely accepted impostors}}{\text{total number of impostors tested}}$$

$$FRR = \frac{\text{total number of falsely rejected authorized users}}{\text{total number of authorized users tested}}$$



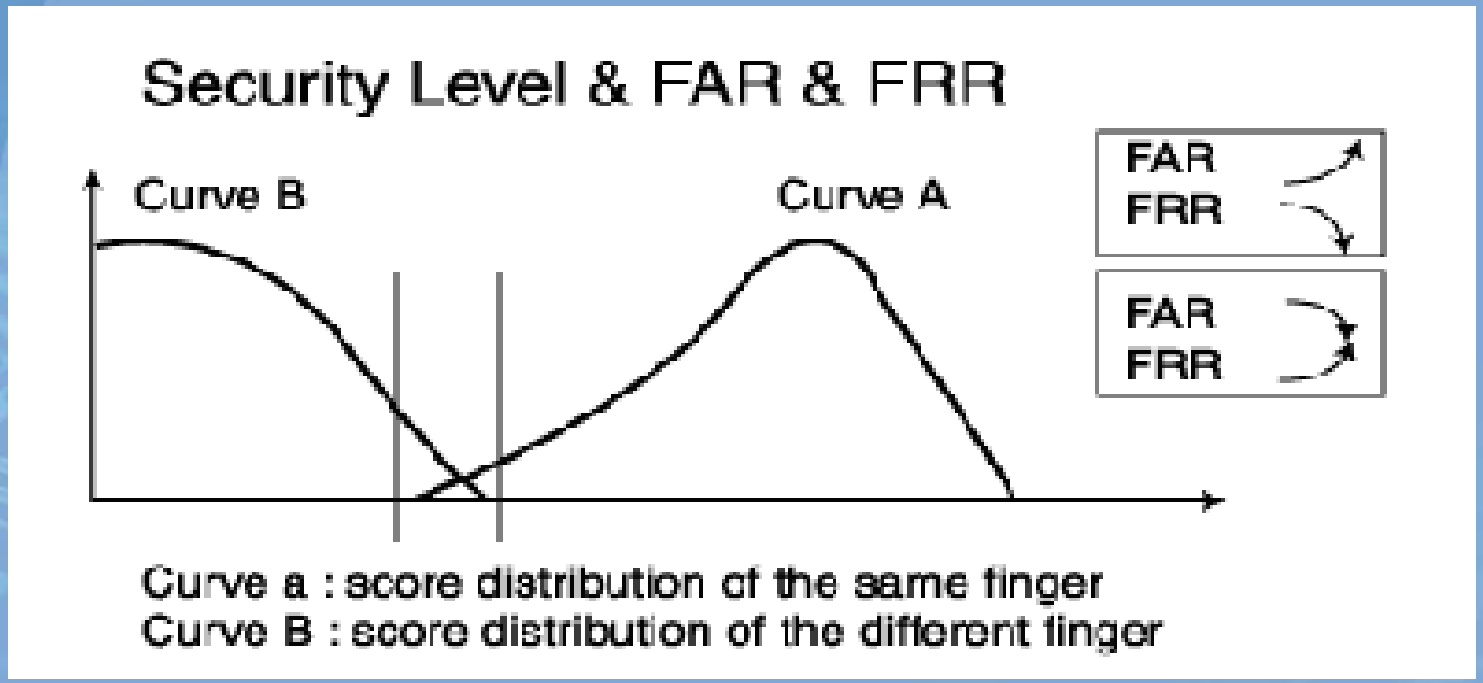
Tasa de Falsos Rechazos (FRR)



Tasa de Falsas Aceptaciones (FAR)

Fuente: D. Maltoni et al., op. cit

Jugando con los umbrales



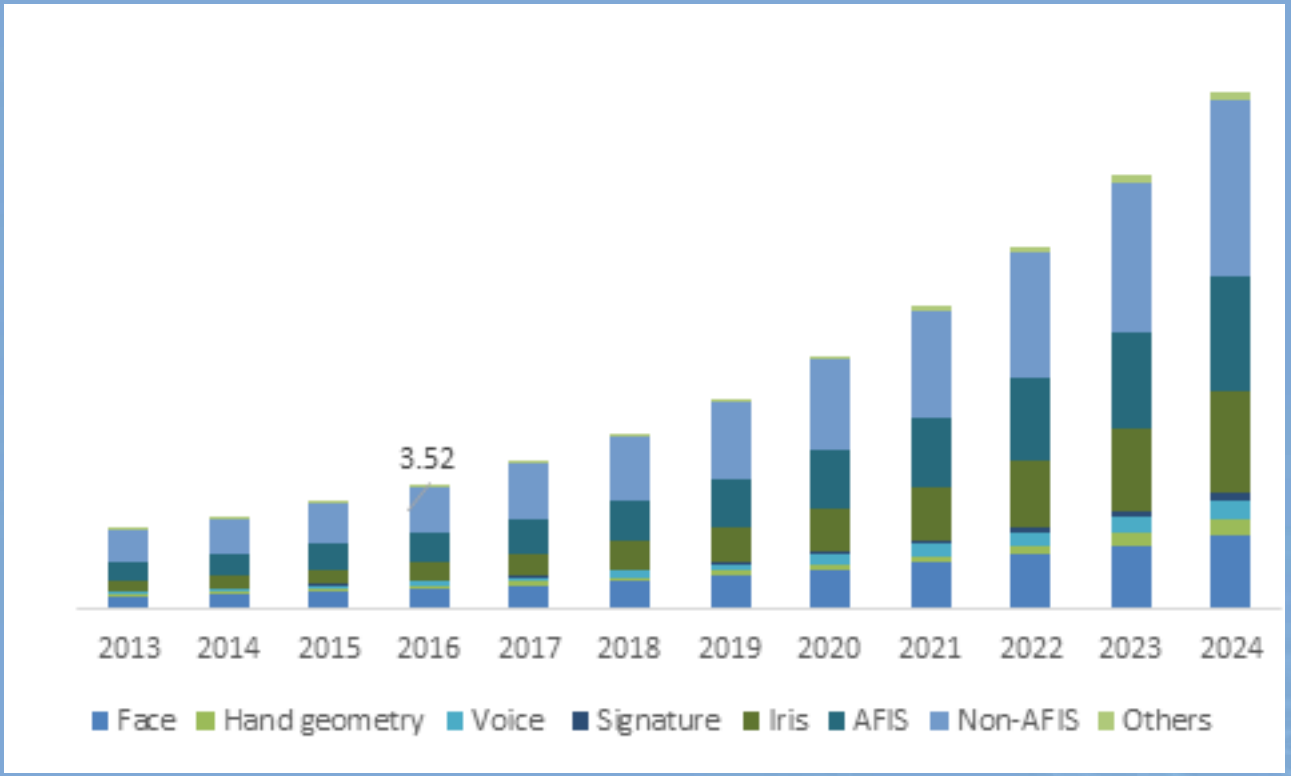
Consideraciones importantes

- Con umbrales más estrechos (más restrictivos)
  - Aumenta la Tasa de Falsos Rechazos
  - Disminuye la Tasa de Falsas Aceptaciones
- Con umbrales más generosos
  - Disminuye la Tasa de Falsos Rechazos
  - Aumenta la Tasa de Falsas Aceptaciones

- La definición de los rangos adecuados depende de:
  - Modelo de Negocios y de Riesgo
  - Modelo de Operación

Mercado de la Biometría

U.S. Biometrics Market Size, By Product, 2013 – 2024 (USD Billion)



Fuente: https://www.gminsights.com/industry-analysis/biometrics-market

Mercado de la Biometría

Biometrics Market Share By Product (2015)

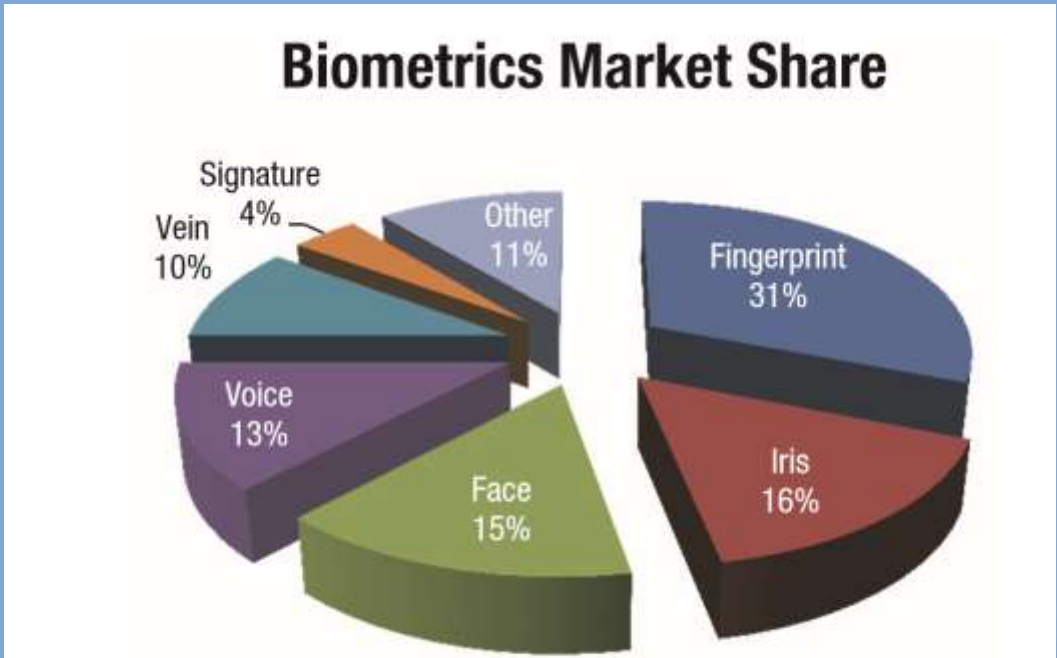
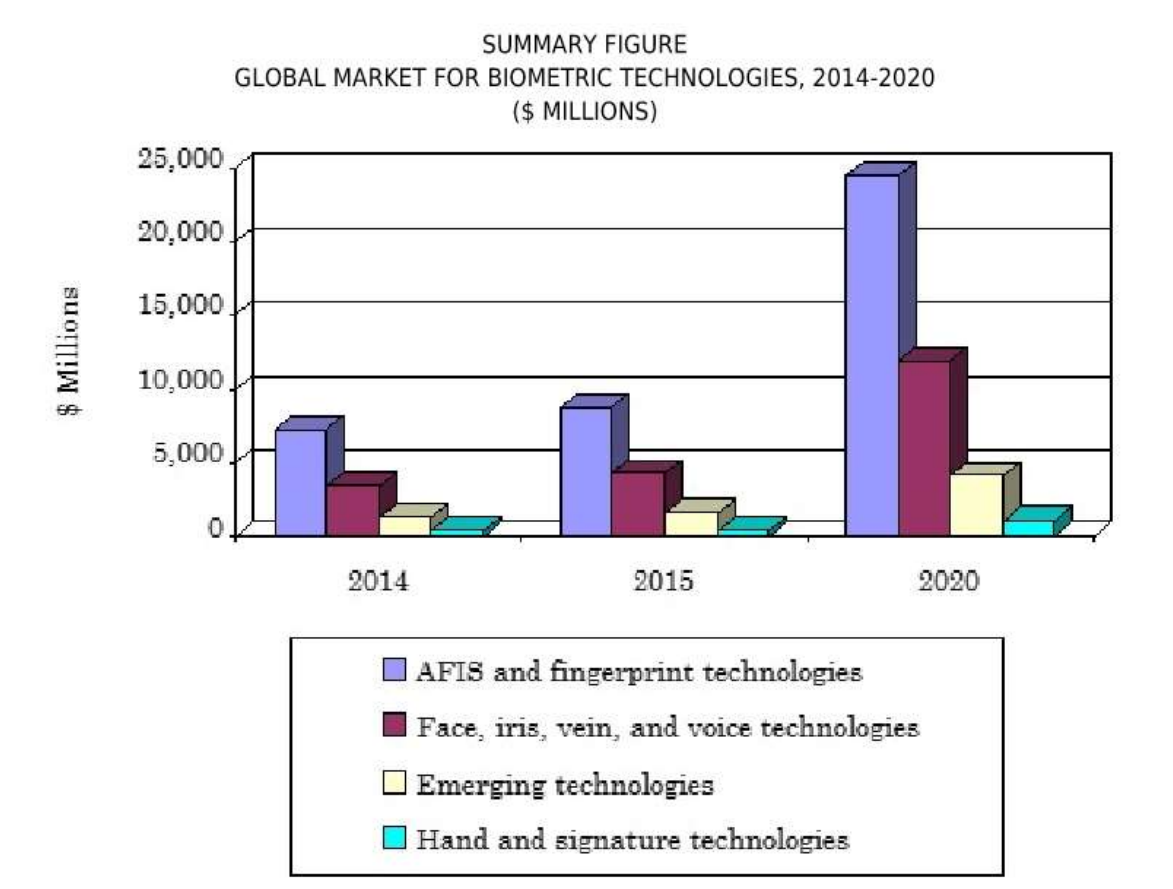


Figure 1: Biometrics market share by system type

Fuente: http://www.ti.com/lit/wp/spry289/spry289.pdf

Mercado de la Biometría



Source: BCC Research

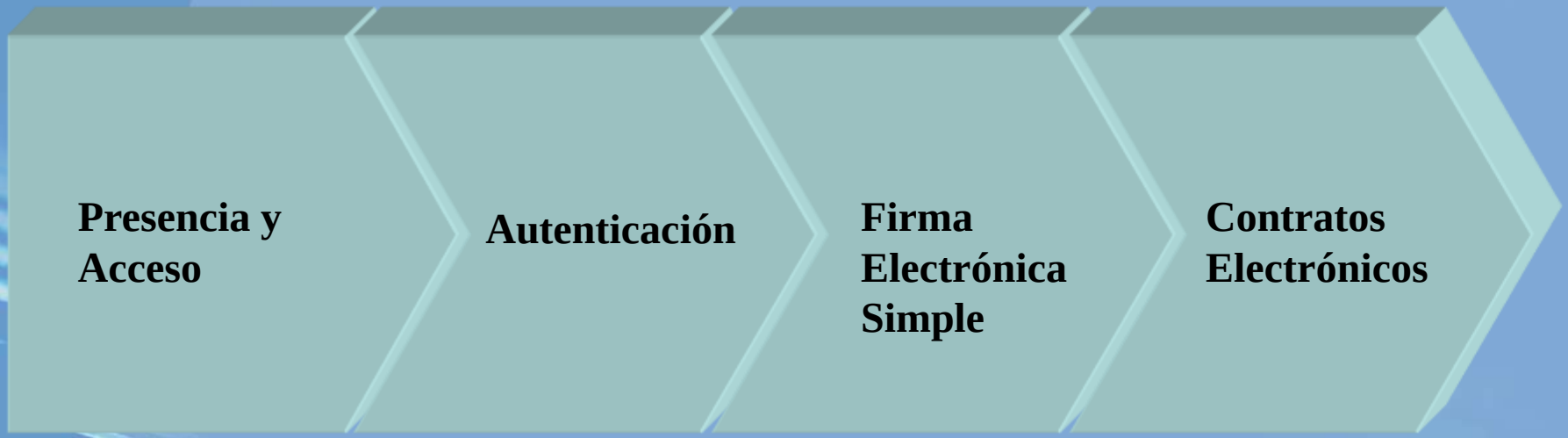
Porqué de la Biometría
Justificación de Negocios

- Variables de justificación
  - Suplantación
  - Identity Theft
  - Bajo costo de operación
  - Modelo de operación simple
  - Ahorro en procesos de Pre y Post validación
  - Transportabilidad
  - Velocidad
  - Moda

Lo que el mercado chileno ha aprendido sobre biometría

Desde	Hacia
Preservar Seguridad	Asegurar Confianza
Disminuir Riesgo	Eficiencia operacional
Complejidad tecnológica	Operación simple
Soluciones aisladas	Plataformas integradas
Enrolamiento libre	Terceros confiables
Precio	Valor

Cadena de valor de la biometría



- Control de Asistencia
- Accesos Físicos y Lógicos

- Verificación de Identidad
- Single Sign On

- Anexos de Contratos
- Medio de Prueba Simple

- Operaciones integrales
- Medios de Prueba Irrevocables
- Firma Electrónica Biométrica

Conclusiones

- Es un espacio tecnológico de alto movimiento
- La tecnología biométrica no es una “bala de plata”: es un medio
- Requiere una mirada de largo plazo, con drivers de negocio claros y medibles
- Su uso efectivo requiere comprensión profunda de:
  - Modelo de negocio
  - Riesgos y Costos de Operación
  - Transformaciones requeridas
  - Tecnologías pertinentes

Téngase presente

- El uso real recomienda uso de biometrías estáticas
  - Considerando el universo de usuarios y el entorno
  - Y que en entornos controlados además permita identificación
- Definir alcance: identificación vs. verificación de identidad
- Justificar económicamente
  - Hint: Sustitución de costos de operación
- Aprovechar al máximo los modelos regulatorios
  - Contratos de adhesión
- Biometría es un mecanismo de verificación de identidad. No resuelve la cadena de seguridad completa.

Anexos

Biometría de Huella Digital

Elementos básicos …

© Marco A. Zúñiga – marco@maz.cl

Diciembre 2006

Datos útiles

- Orígenes se remontan a usos forenses, fines siglo XIX
- La comparación de Huellas Digitales tradicionalmente se basa en la comparación de los puntos característicos de una Huella Digital – minucias
- Los procesos manuales son realizados por Peritos Dactiloscópicos
  - Procesos no triviales de búsqueda y match, con alto entrenamiento
- Existen distintas formas de capturar las huellas digitales
  - Huellas latentes, huellas patentes, mecanismos electrónicos
  - Una huella patente (tinta) se puede escanear muy bien
- No se ha encontrado un par de huellas digitales iguales
  - Incluso entre gemelos univitelinos
- No se modifican durante toda la vida
  - Pero se borran o destruyen, y los niños las tienen “chiquitas”

Puntos Característicos (Minucias)

Características de las Minucias

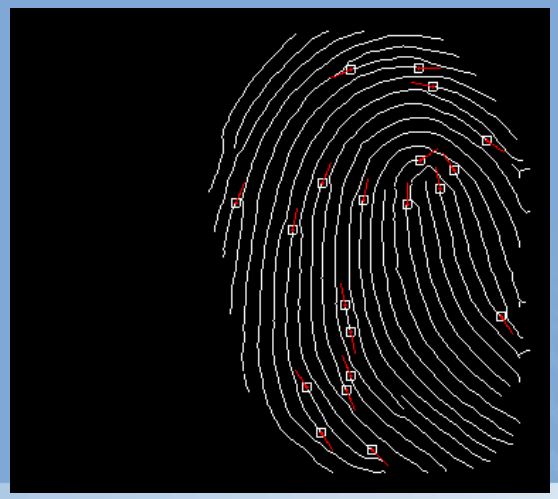
- Existen 7 tipos de puntos de minucias y 4 orientaciones de huellas
- Típicamente podemos encontrar 60 a 120 puntos por huella.
- 12 puntos bastan para identificar.
- El patrón de identificación corresponde a un vector que se extrae en base al análisis de las características de cada huella dactilar:
  - Tipo
  - Posición
  - Angulo

Procesos Genéricos con Huella Digital

Captura

Esqueletización

Afinamiento



Extracción de Minucias

Proceso General

- Enrolar
  - Almacenar patrón de huella asociado a una Identidad
- ¿Verificar Identidad?
  - Capturar “identidad + imagen de huella”
  - Comparar “imagen de huella” con “patrón almacenado” asociado a la “identidad”
- ¿Identificar?
  - Capturar “imagen de huella”
  - Encontrar “identidad” a partir de los “patrones almacenados”
- ¡¡¡WARNING!!!
  - Existen muchos parámetros de diseño de ingeniería de detalle no triviales, y específicos para cada caso

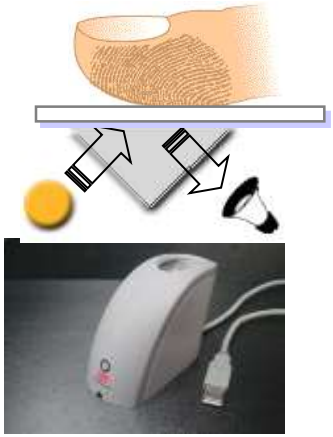
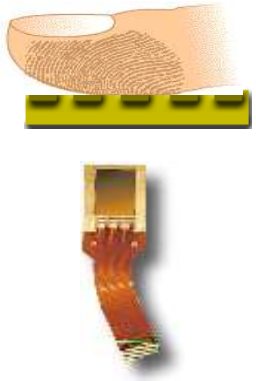
Algunas preguntas de Ingeniería

- Qué tipo de sensor usar
  - Calidad, precio, ambiente, usuarios, plataformas, autonomía, suplantación, flexibilidad, tiempo de respuesta, etc.
- Qué almacenar en la BD
  - Imágenes de huella, minucias propietarias, minucias estándar
- Qué BD y cómo
  - Local, distribuida, centralizada, alta disponibilidad, seguridad, protección
- Cómo comparar
  - Qué algoritmo usar, velocidad, calidad, umbrales
- Recursos de procesamiento, cálculo y análisis
- Dónde integrar
  - Plataforma, aplicación tiempo de respuesta, distribución, seguridad
- Modelos de Operación
- Marco normativo regulatorio
- Interoperabilidad

Capturando Imágenes de Huella

- Requerimientos mínimos hoy
  - Resolución 500 dpi o más
  - Escala de grises en 8 bits
  - No aceptar deformación (para interoperabilidad)

Tecnologías de Lectura de Impresiones de Huella Digital

Classification	Optical	Semiconductor	Light Emitting
Method			
Strength & Weakness	▪ Strong Endurance ▪ Additional Light and Prism needed – Additional Expense ▪ Poor Recognition for the dry ▪ Weak for Hacking	▪ Mass production & cheap price ▪ Poor Recognition for the dry ▪ Weak for ESD and Impact ▪ Easy corrosion	▪ **Strong Endurance (over 1.5M touch)** ▪ High Security ▪ Simple Structure ▪ Good at dry fingerprint ▪ Cheap price
Manufacturer	Nitzen(Korea)	Verdicom(U.S), Authentec(U.S) etc.	Testech.

El tema del almacenamiento

- Las imágenes de Huella Digital son MUY pesadas y MUY complejas (alta entropía)
  - BMP, RAW – 250+ Kb por imagen
  - JPG y GIF “matan” las huellas (además que comprimen 1:3)
- Solución: WSQ (Wavelet Scalar Quantization) (1:15 y más)

Imagen reconstruida de JPEG

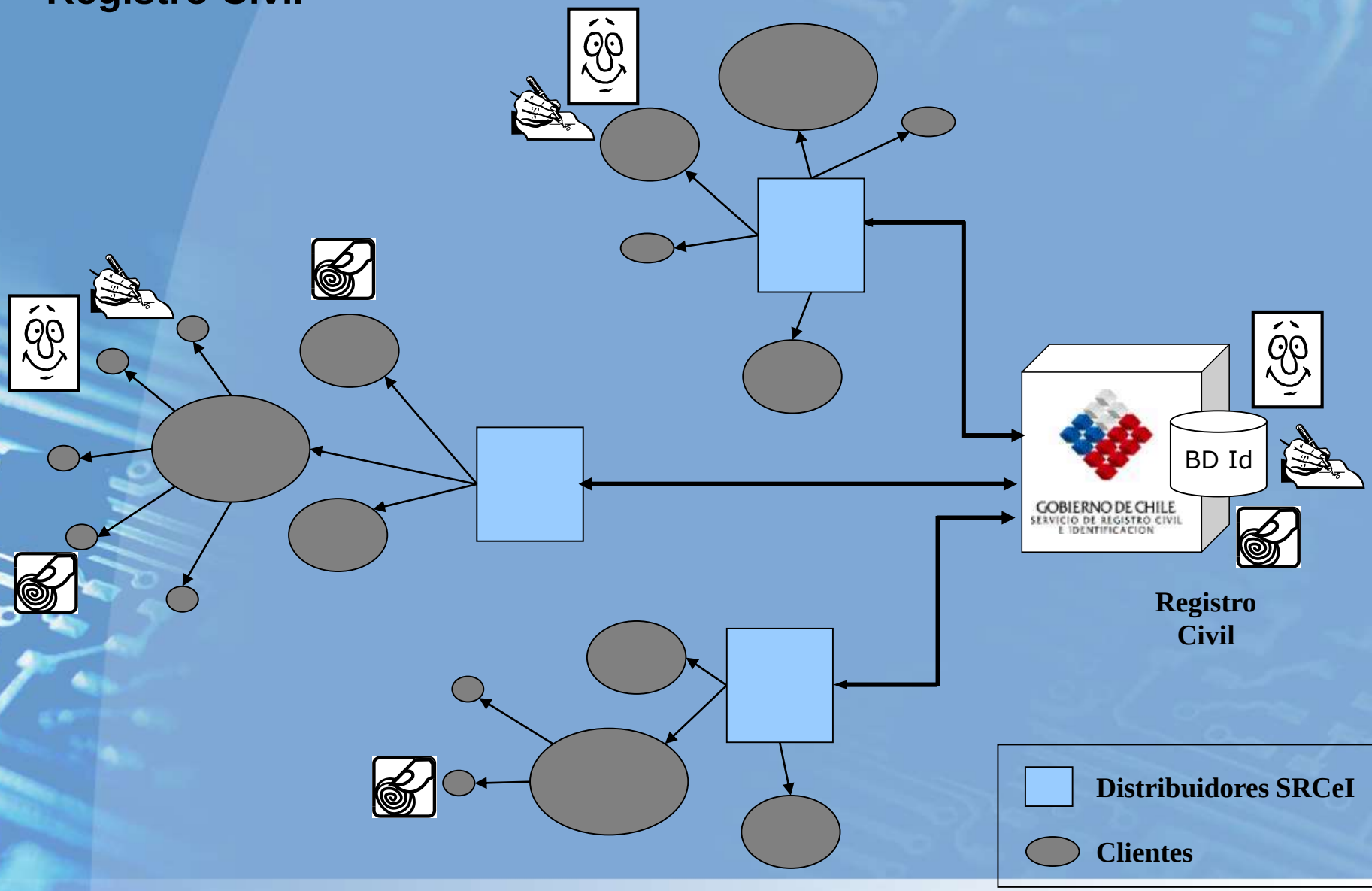
Imagen reconstruida de WSQ

Proyecto Registro Civil

- Incorpora AFIS (Automatic Fingerprint Identification System) en la Cédula de Identidad y en la Base de Datos de Registro Civil

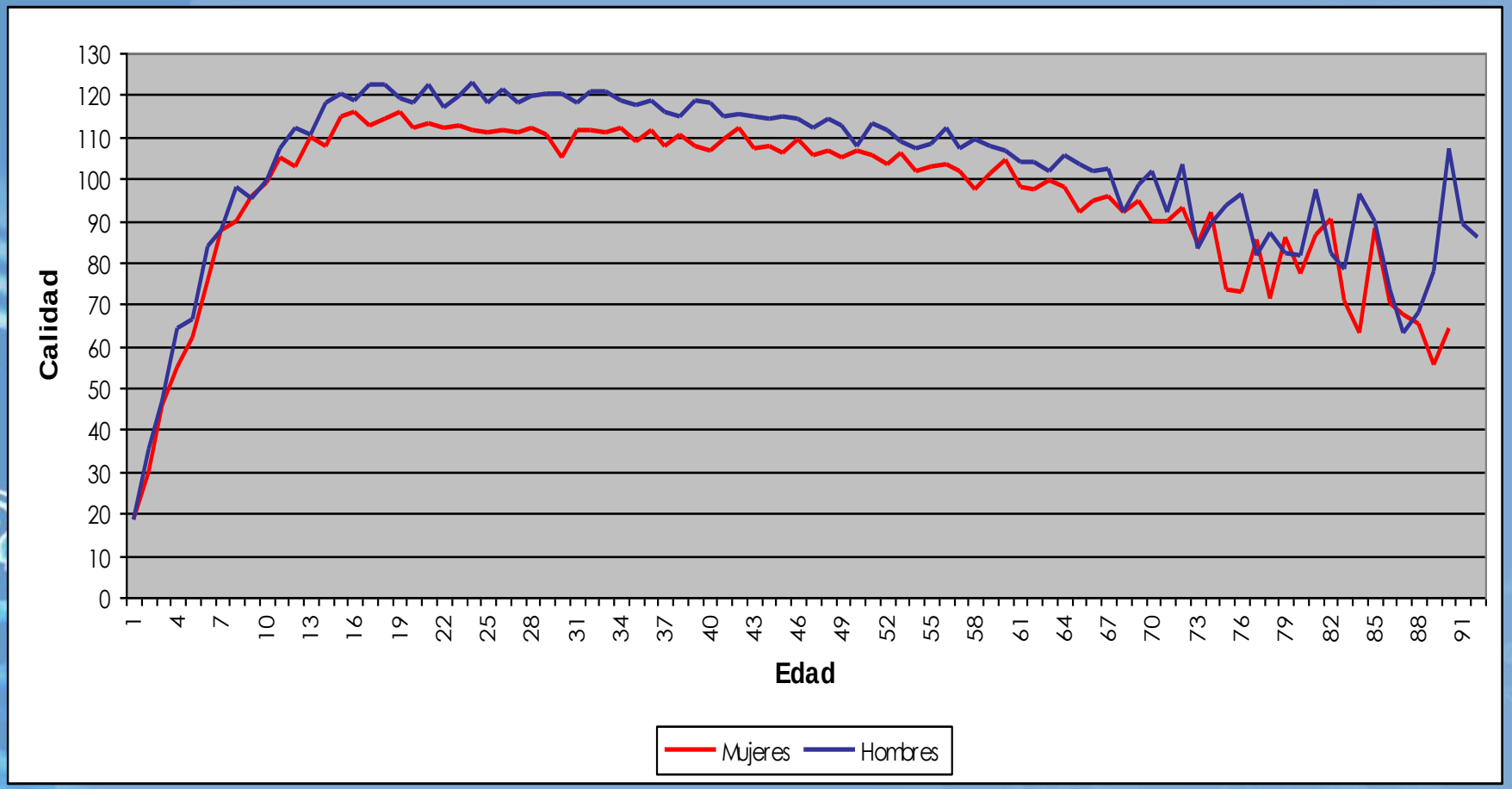
- Permite:
  - Verificación con Huella Viva contra cédula (1:1) en forma autónoma
  - Recuperación de datos desde BD Registro Civil en Línea (WS)

Modelo de Servicios de Identificación
Registro Civil



Estado actual: AFIS 1:1

Calidad de la imagen según la edad



Fuente: Servicio Registro Civil e Identificación

Casos de Uso Biometría Huella Digital

Protección de Estaciones	Entrega de Valorados
Login Seguro, Protección de Claves, Encriptación Archivos	Verificación de identidad Talonarios, Vales Vista, Cheques según monto
Verificación de Identidad	**Autenticación Remota**
Apertura de Cuentas Verificación de Clientes Seguridad Ciudadana	Aplicaciones WEB Firma Electrónica Autenticación ATMs

La Biometría mejora los procesos donde la identificación es factor crítico

Casos de Uso y Operación Real
Modelos de Arquitectura de Solución
Aspectos a Considerar

Marco A. Zúñiga – marco@maz.cl

Comentario y Corolario de Experiencia:

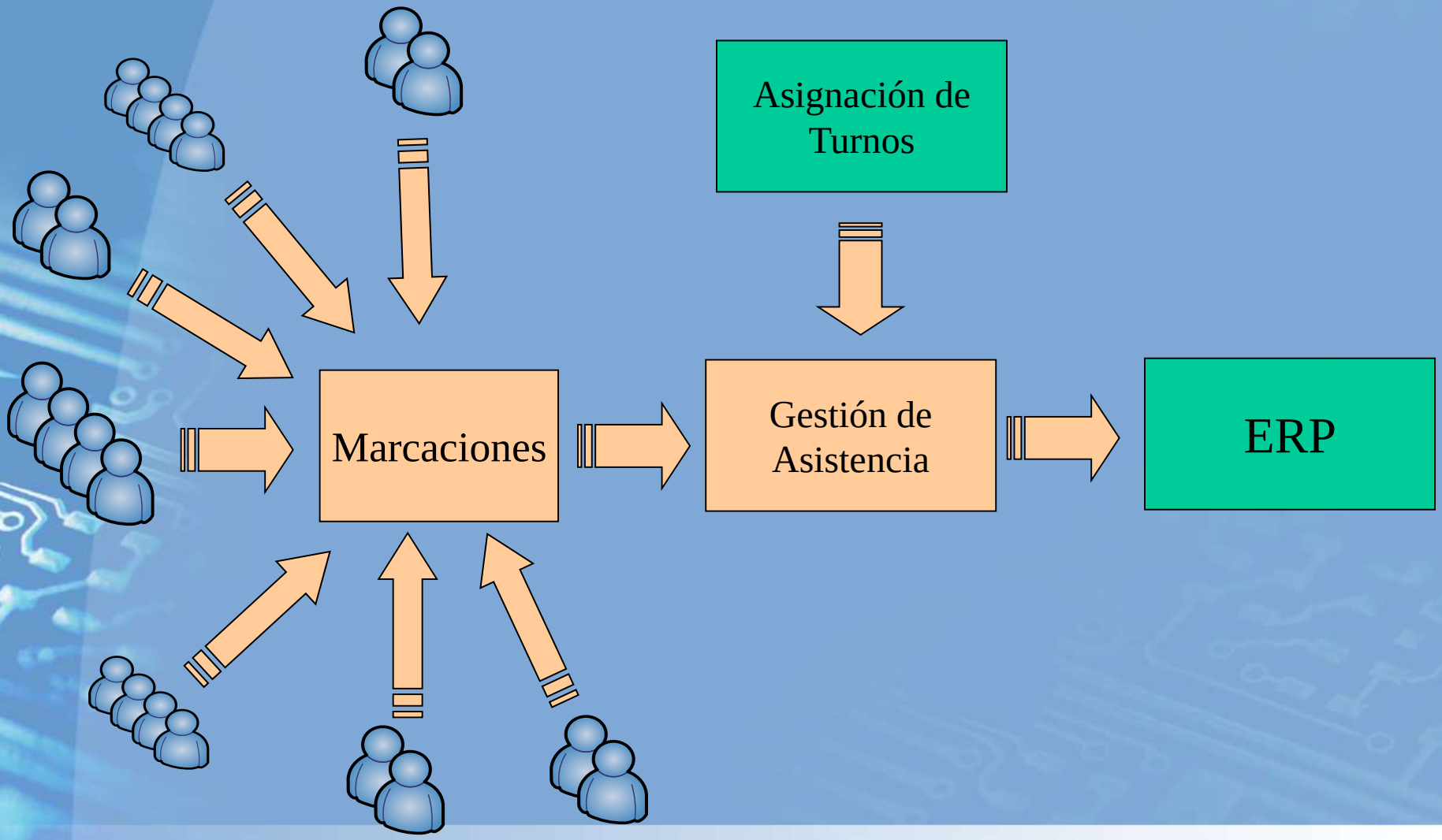
A escala pequeña, cualquier tecnología funciona.

En condiciones de restricción más severas, por muy simple que sea, es complejo. Y ahí son importantes los parámetros de Ingeniería.

Caso 1: Control de Asistencia

- Soluciones Actuales
  - Libro de Asistencia
  - Tarjetas Magnéticas
  - Tarjetas de Proximidad
- Requerimientos de la Inspección del Trabajo
- Identificación de complejidades
  - ¿Turnos de más de 24 horas?
    ¿Asignaciones rotatorias?

Arquitectura Global Gestión de Asistencia



Control de Asistencia: Alternativas Biométricas

- Requerimientos:
  - Entradas, Salidas, Colación, Presencia
- Alternativas
  - Dispositivos Autónomos
  - Dispositivos en línea
- Problemas
  - Puntos de alto tráfico, puntos de bajo tráfico
- Componentes de Arquitectura
- Discusión de Casos de Uso

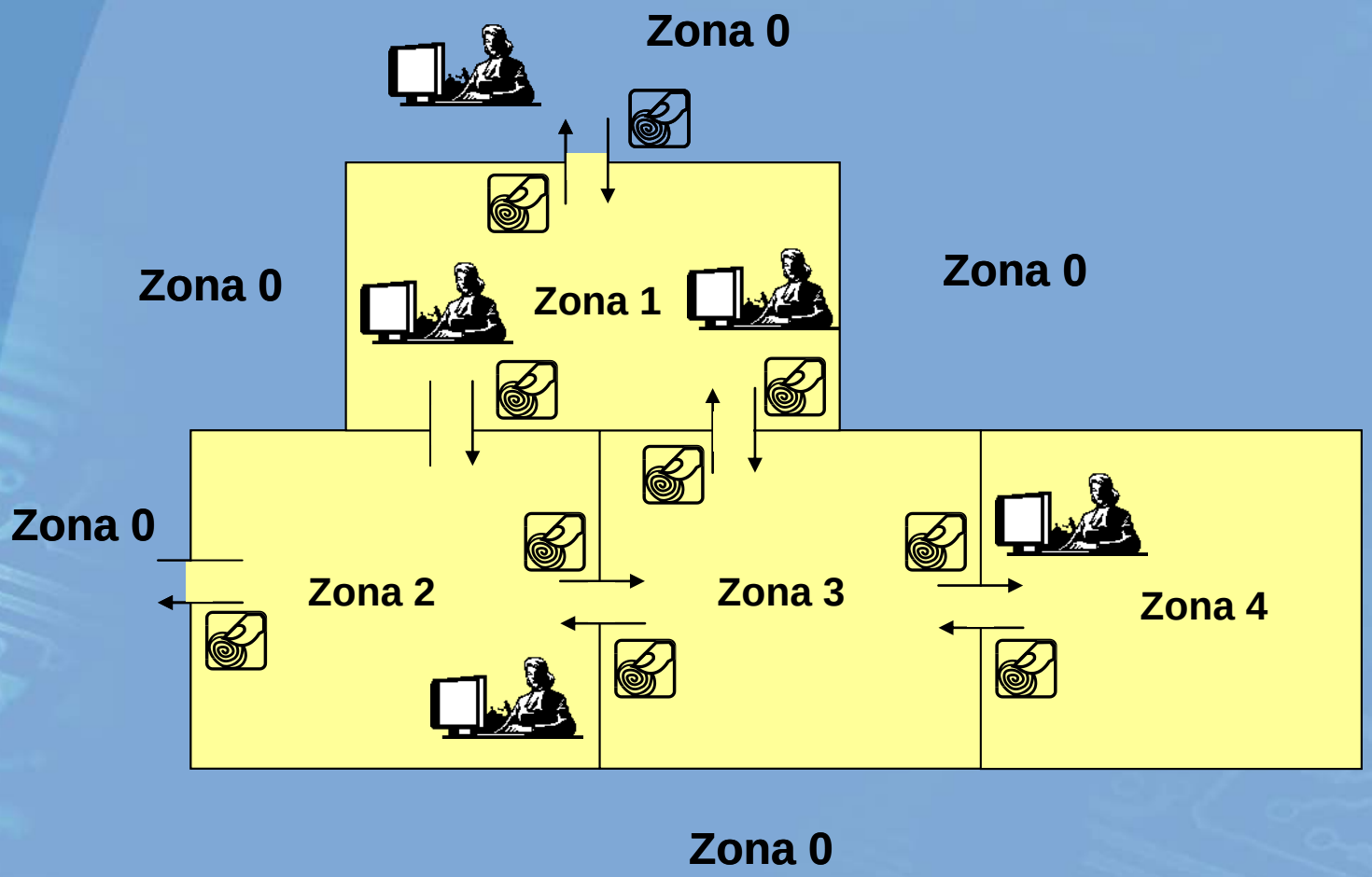
Ejercicio Práctico

- Arquitecture, genere alternativas e identifique costos aproximados para las siguientes soluciones de Control de Asistencia:
  - Empresa de 70 empleados, un acceso, un recinto, turnos administrativos y variables
  - Cadena de tiendas distribuidas, 40 empleados, 10 tiendas
  - Empresa de 1.500 empleados, 100 puntos distribuidos, 1 matriz
  - Faenas mineras
  - Guardias de Seguridad con Rondas
  - Caso ING

Caso 2: Control de Acceso

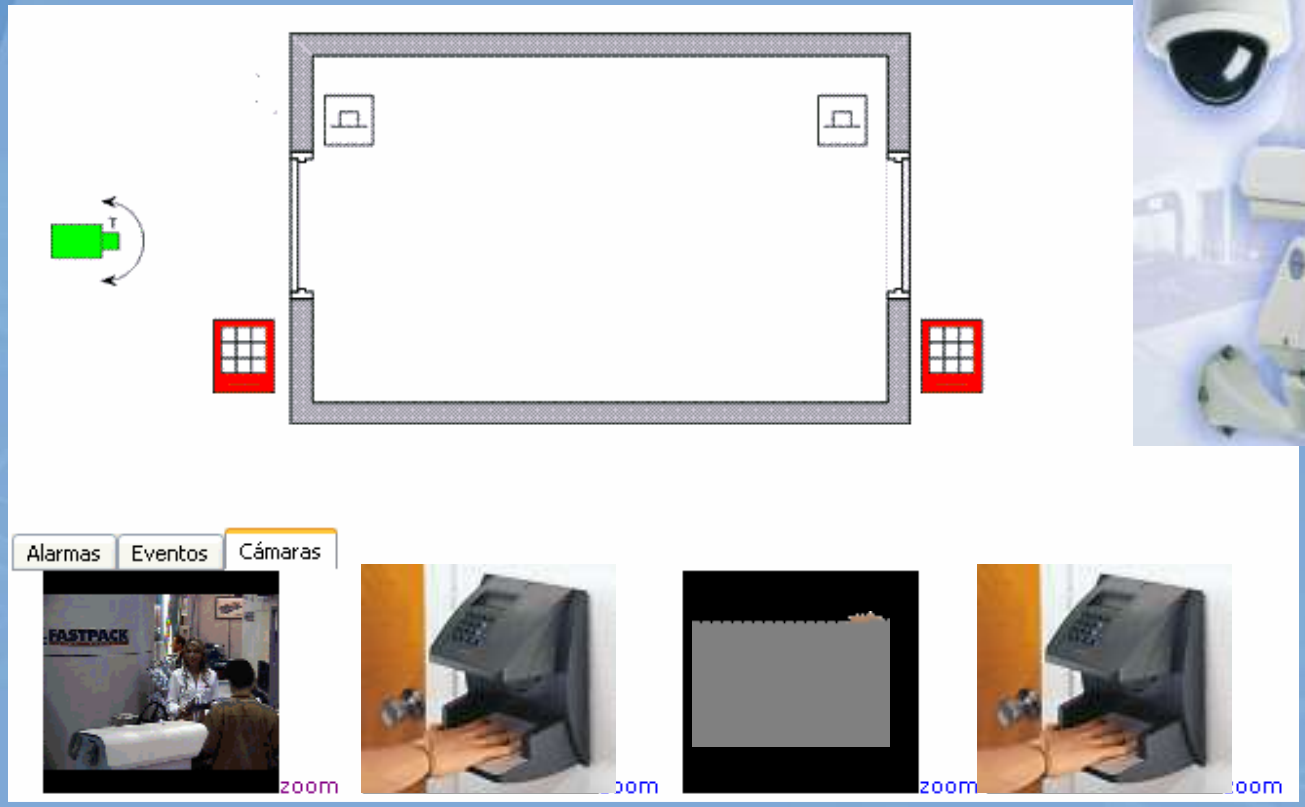
- Solución tradicional:
  - Tarjetas de Identificación
  - Tarjetas Magnéticas
  - Dispositivos de Proximidad
- Componentes:
  - Identificación
  - Verificación
  - Manejo de Chapas y Apertura
- Tiempos de respuesta

Control de Acceso: Ejemplo



Pregunta: ¿Anti Pass Back? ¿Cómo?

Aplicación compleja: Biometría + CCTV



Caso de Negocios: Codelco – El Teniente

Control de Visitas y Eventos

- Temas a resolver:
  - Frecuencia
  - Identificador
  - Tiempo de Respuesta
  - Pasaportes temporales
  - Listas Blancas y Listas Negras

Ejercicio Práctico

- Arquitecture, genere alternativas e identifique costos aproximados para las siguientes soluciones de Control de Acceso:
  - Datacenter con 20 empleados autorizados
  - Caso ING
  - Planta Industrial
  - Edificio Birmann para visitas
  - Escuela de Ingeniería Universidad de Chile
  - Ministerio de Economía
  - Bóveda del Banco Central

Elementos a considerar Verificación de Identidad

- Ambitos:
  - Verificación de Identidad Remota
  - Autoatención
  - Persona a Persona
- Restricciones Técnicas
  - 1:1, 1:n
  - Base de Datos? Replicación?
  - Plataformas soportadas
  - Modelo de Integración

Aspectos legales

- Marco Ley 19.628: ¿De quién es la Base de Datos?
- Usos y aplicaciones
- Respaldo y soporte legal
  - Sirve como Firma Electrónica? (Ley 19.799)
  - Diferencias Sector Público y Sector Privado

Caso 3: Verificación de Identidad de Clientes

- Soluciones Actuales
  - Revisión de Documentos de Identidad
  - Tarjetas de Banda Magnética (1 o 2 de 3)
  - Múltiples procesos de pre y post validación
  - Riesgo de las operaciones?
  - Costo de las operaciones?
- Pregunta: ¿Cuál es la principal justificación para incorporar biometría?
- Caso FFIEC / USA

Ejercicio Práctico

- Arquitecture, genere alternativas e identifique costos aproximados para las siguientes soluciones de Verificación de Identidad de Clientes:
  - Isapres
  - Red de ATMs
  - Tarjeta Bancaria y Plataforma de Atención de Clientes
  - Plataforma de Atención de Cajas de un Retail
  - Soporte de identidad para medios de Pago Abiertos

Otros casos

- Single Sign On para aplicaciones
- Contratos Electrónicos
- Forensic
- Acceso a dispositivos
- Domótica (por ejemplo, chapas biométricas)
- Servicios sobre Internet

Tecnologías biométricas dominantes

Geometría de la Mano
Handkey

Dispositivos de Huella

Lectura del Iris

- Alternativas de Dispositivos:
  - Host Based
    - Típico Uso: Verificación de Identidad para aplicaciones (multiuso)
  - Autónomos
    - Típico uso: Control de Asistencia y Control de Acceso

Factores Críticos para la Selección de una Tecnología Biométrica

- Requerimientos Básicos
  - Universalidad
  - Distinguibilidad
  - Permanencia
  - Colectabilidad (cuantitativo)
- Requerimientos prácticos de Implementación
  - Desempeño
  - Aceptación
  - Circunvención (capacidad de fraude)

Fuente:

D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar
Handbook of Fingerprint Recognition
Springer, New York, 2003

Comparación Cualitativa entre Tecnologías de Autenticación

* Score : 1 (High) , 6 (Low)

classification	Key	ID Card	Guard	Voice	Retina	Hand	Fingerprint
Duplication	1	2	2	1	6	3	6
Inconvenience	5	4	4	2	1	4	6
Speed	4	4	1	3	2	4	5
Risk of Loss	1	1	5	6	6	6	6
Purchasing	5	5	1	5	5	5	6
Stained	6	6	6	6	1	2	5
Broken by outside damage	1	1	1	2	2	2	6
Cost of Initial Setting	5	4	1	2	1	3	3
Cost of individual issue	3	5	6	6	6	6	6
Total	31	32	27	33	30	35	49

* Reference : Korea Electronic and Communication Center <Oct. 2001>

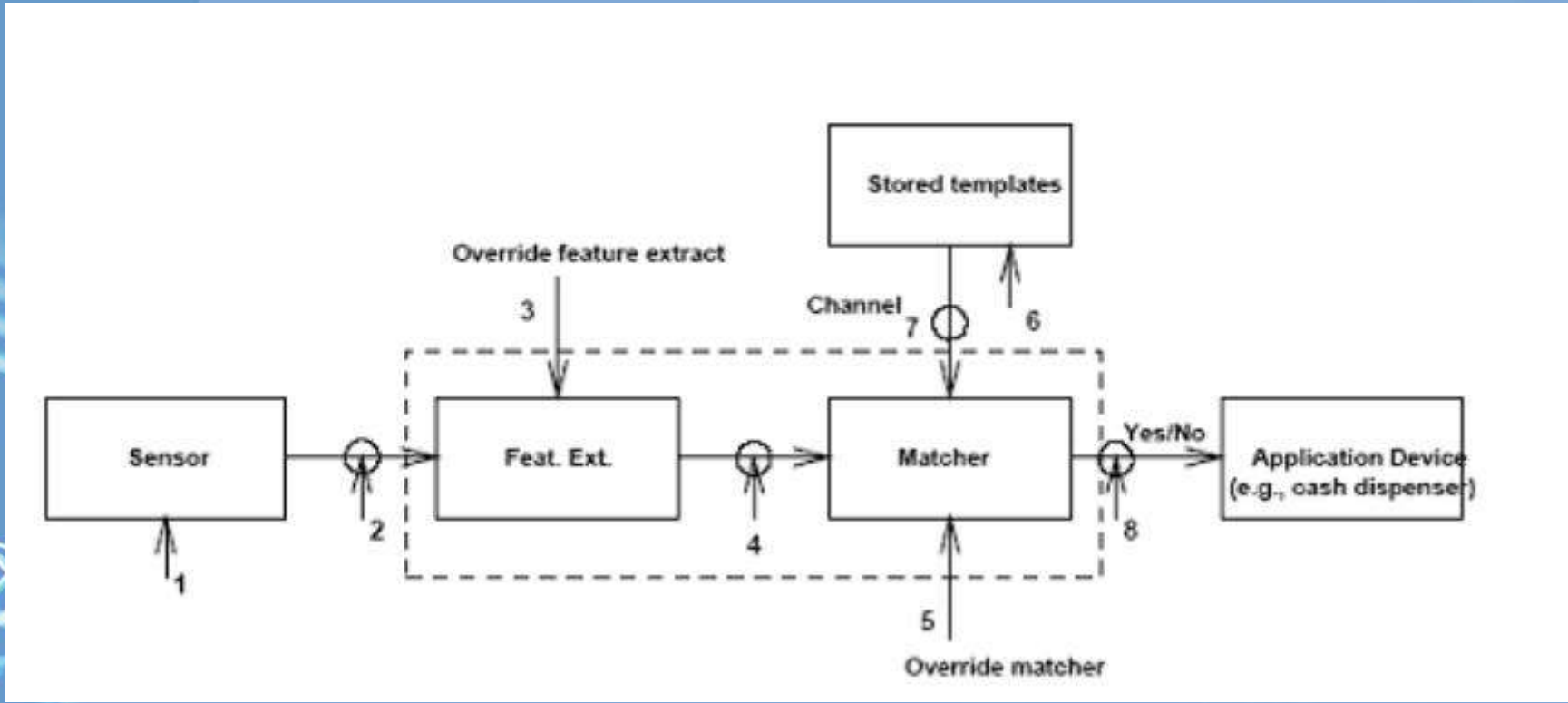
Comparación Cualitativa entre Tecnologías Biométricas

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 1.1. Comparison of biometric technologies. The data are based on the perception of the authors. High, Medium, and Low are denoted by H, M, and L, respectively.

Fuente: D. Maltoni et al., op. cit

Potenciales quiebres de seguridad para verificación de identidad biométrica



Modelo de Ratha, Connel y Bolle

Gracias por su atención

Material Adicional en:

http://www.maz.cl

marco@maz.cl