I/O Software, Inc.

Provider of innovative software solutions

Biometrics

Understanding the Architecture, Standards and API's, Encryption and Authentication Security of Integration into Existing Systems & Applications

National Information Systems Security Conference

William Saito

President/CEO

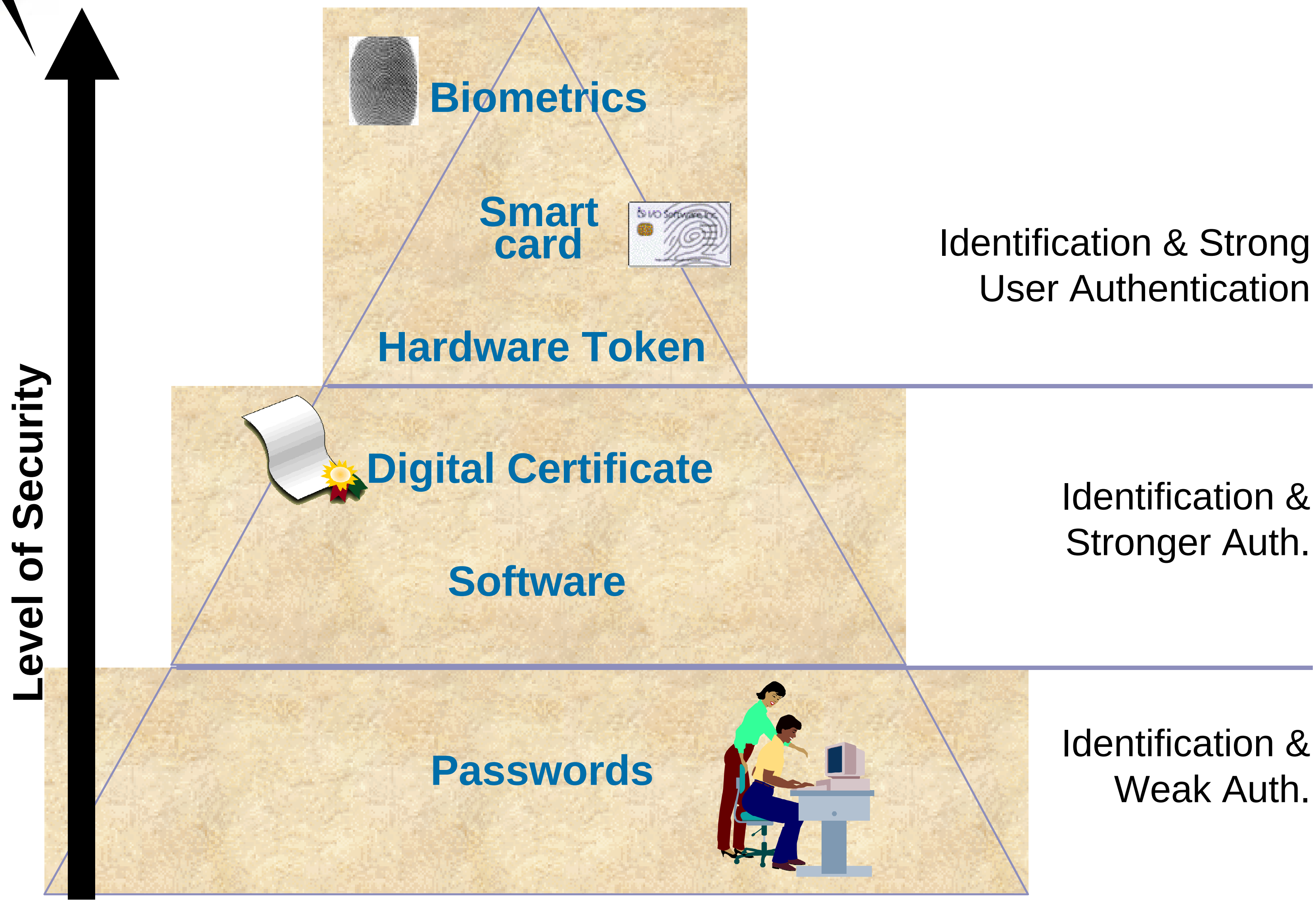
Company

- Founded in 1991
- Core Products & Technology
  - Biometric driver development & integration
  - Commercial biometric application development
  - Biometric solution provider
- Original developer of BAPI & BioAPI Chair
- Licensed to biometric technology to Microsoft
  - BAPI & SecureCore

Biometrics 101

Choosing your biometric technology

Authentication devices



Identification & Strong User Authentication

Identification & Stronger Auth.

Identification & Weak Auth.

Why are biometrics important?

- What you know (i.e., password or PIN)
  - Insecure, can be forgotten, needs to be changed, can easily be copied or given to others
- What you have (i.e., ID card or key)
  - Can be lost or copied (without your knowledge), replacement costs are high
- What you are (i.e., fingerprints)
  - Only non-reputable authentication method. Conclusively proves you are who you say you are

Types of biometrics

- Physiological vs. behavioral characteristics
  - Physiological: Don’t change over time
    (Fingerprint, hand, iris, etc..)
  - Behavior: Change over time
    (Voice, signature)
- Interactive vs. Passive biometrics
  - Passive: Facial

Types of biometrics

- Fingerprint/Finger length
- Hand geometry
- Iris/Retina
- Facial image/Facial thermograms

- Voice
- Signature
- Keystroke

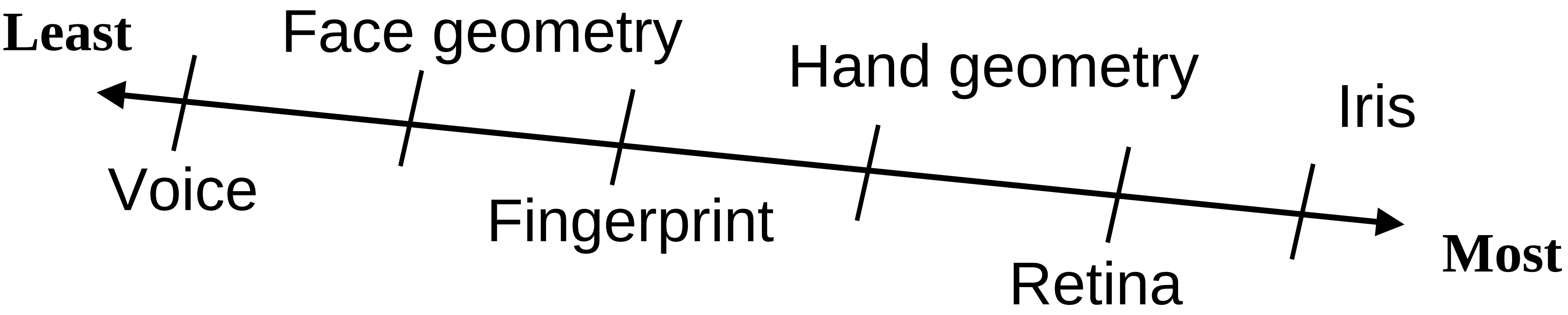
Trade offs

- Cost
- Security
- Size
- Convenience
- Speed
- Accuracy
- Connectivity & compatibility (ports/OS/CPU)
- *Intrusiveness*

Costs differ

Device + Integration + Software + Training + Enrollment + Maintenance + Support

Expense



Least

Voice

Face geometry

Fingerprint

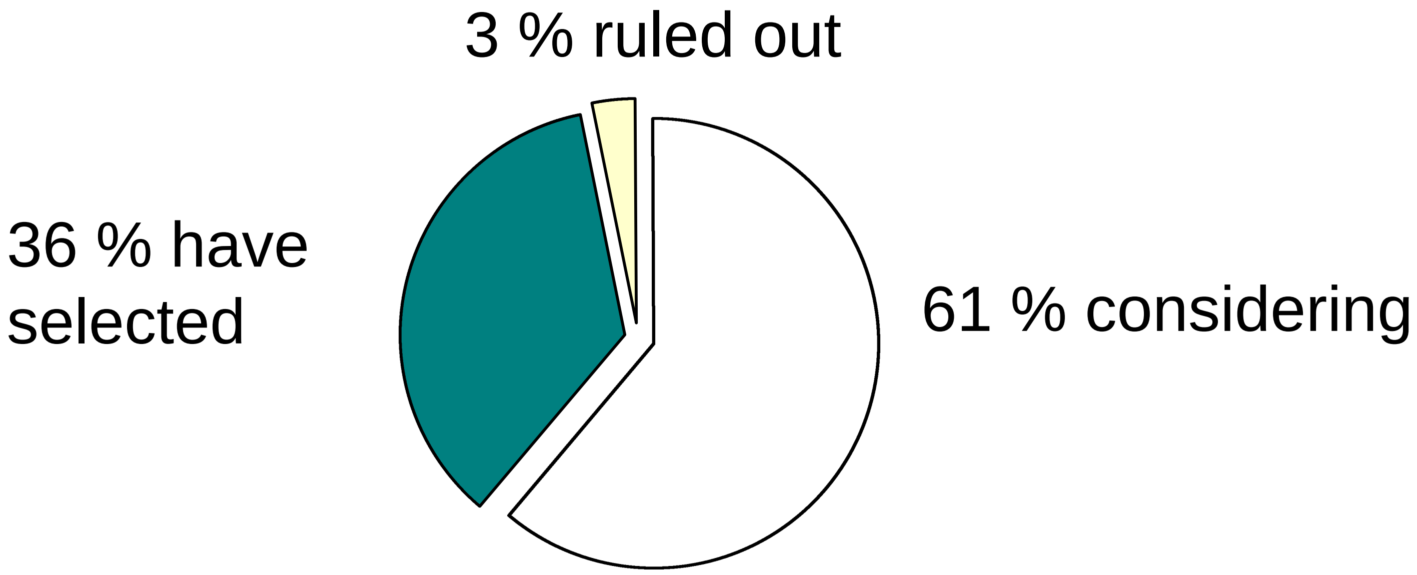
Hand geometry

Retina

Iris

Most

Current status



*Source: Information Week, “Biometrics Survey”, February 1999

Who’s using biometrics

- Secure access
  - Nationwide
  - Barclay’s Bank
  - Citibank
  - NSA/CIA
  - Various corporations
- Convenience
  - INSPass
  - CanPass
- Preventing fraud
  - Mr. Payroll
  - CT Dept. of Social Services
  - Acroprint
- Protecting lives
  - O’Hare Airport
  - Pyxis

User acceptance is key

- Some biometrics discriminate
  - Fingerprint: skin and race effects
  - Face: beards, photographs trick
  - Voice: colds, sore throat affect accuracy
- Can you afford…
  - a false reject or a false accept?
  - to offend a valued customer?
- Minimal level of effort required for acceptance

Biometric taxonomy

• Cooperative	vs. Non-cooperative
• Overt	vs. Covert
• Habituated	vs. Non-habituated
• Supervised	vs. Unsupervised
• Stable Environment	vs. Unstable
• Optional	vs. Mandatory

Biometrics do best in conditions of left column

How biometric devices work

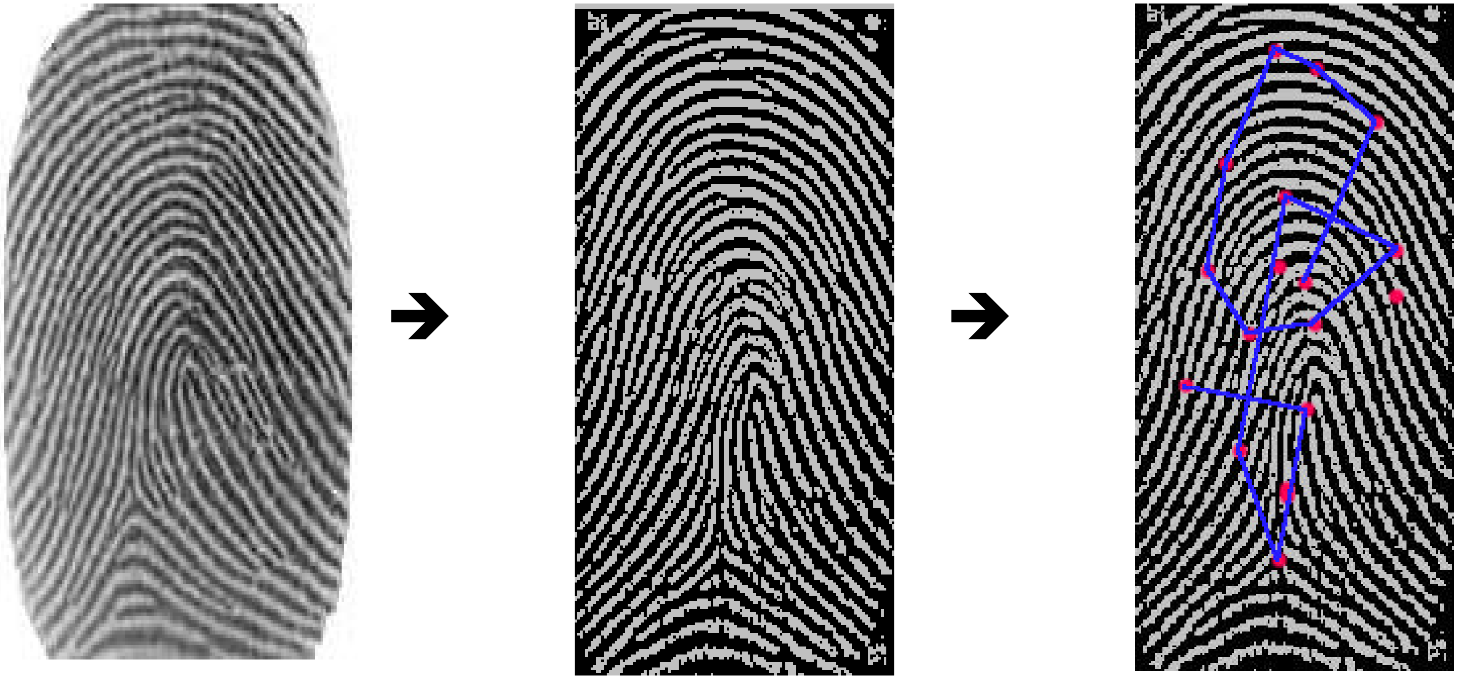
How biometrics work

- User enrollment
- Image capture
- Image processing
- Feature extraction
- Comparison
  - Verification
  - Identification

Templates

- Templates are usually not compatible between vendors
- Template size/type varies
  - 50 - 8000+ bytes
  - Speed vs. accuracy vs. size
- Template types include:
  - Vectors
  - Minutiae

Image conversion



“Raw” Data

Processed Data

Template Data

Comparison methods

- Verification
  - 1:1 matching
  - To verify that the person is who he says he is
- Identification
  - 1:n search
  - To find a person out of many in a database

Types of devices

Device interfaces

- Various port types (and issues)
  - Composite video signal
  - Parallel port (Pass through & ECP/EPP modes)
  - Serial port (RS-232, RS-422, RS-485, etc..)
  - USB port (NT support)
  - PCMCIA port
  - Weigand
- Transfer time / ease of integration
- Encryption

Image capture component

- Resolution
  - 350 - 500+ dpi
- Sensor types & materials
  - Optical
  - Capacitance
  - Resistance
  - Thermal
  - Polymer

Sensor comparisons

- Optical
  - Most bulky
  - Distortion issues
  - Dry finger problems
- Capacitance
  - ESD issues
  - Surface strength issues
  - Surface area limitations
- Thermal
  - Lowest surface area required

Device sophistication

- Simple
  - Scanner (only)
  - Scanner with encryption
- Processing (self-contained)
  - Scanner with CPU and/or LSI for fingerprint processing
  - Scanner with CPU and memory for storage of fingerprint (optional encryption)
- Complex
  - Scanner + CPU + protected storage for PKI type use

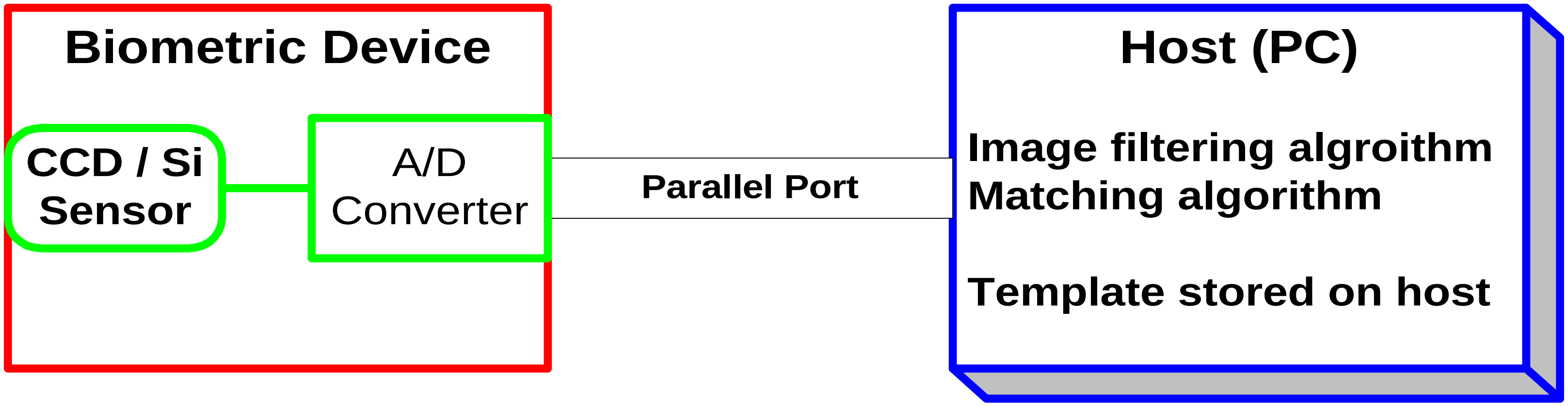
Evolution of biometric devices

1st generation devices

- First Generation
  - Supervised
  - Slow
  - Bulky devices / heavy!
  - Required calibration
  - Not PC based
  - Very expensive! (>$5K)
  - Application: Criminal Enforcement

1st generation devices

- Simple design / low-cost device
- No security
- All processing done on host PC
- Ideal for simple low security applications



Biometric Device

CCD / Si Sensor

A/D Converter

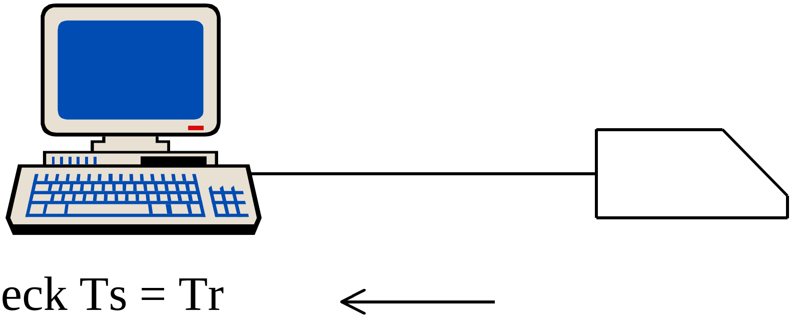
Parallel Port

Host (PC)

Image filtering algroithm
Matching algorithm

Template stored on host

1st generation devices



PC or Server

Fingerprint Unit

Store
K, Tr

Store K
Get Ts

Check Ts = Tr

Ts’ = Enc (Ts by K)

- Need standard
- Key delivery of the symmetric key

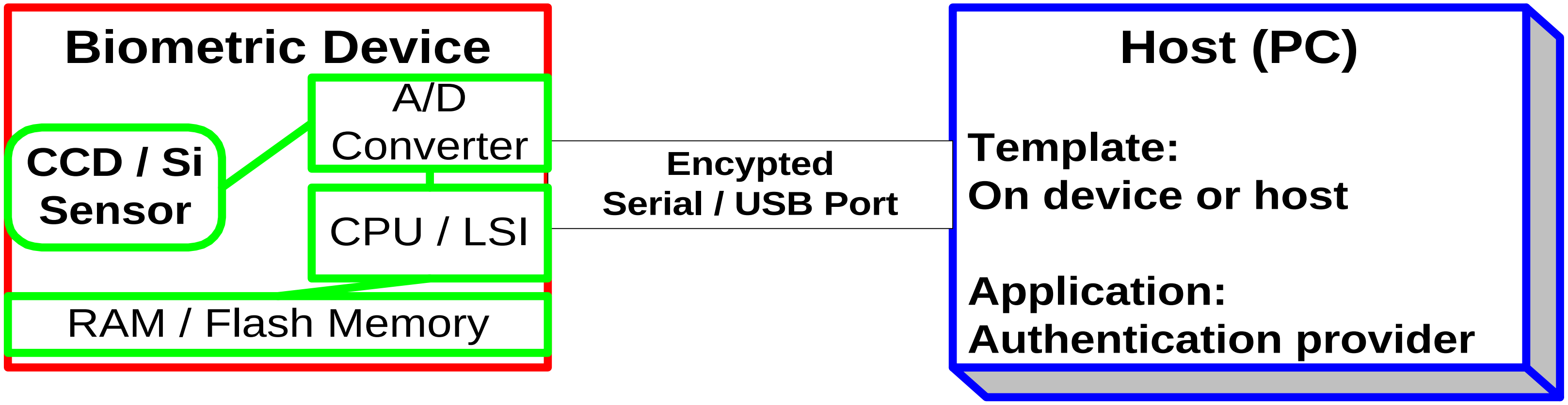
K: Symmetric Key
Tr: Reference Template
Ts: Sample Template

2nd generation devices

- Second Generation
  - Optical only devices
  - High FRR and/or FAR
  - Required some finger preparation
  - Somewhat PC friendly development environment
  - Expensive (>$1K)
  - Applications:
    - Building access control
    - High security computing in vertical applications

2nd generation devices

- Device contains a lot of intelligence
- Communications encrypted to host
- Some or all processing done in device
- Ideal for physical access, smart cards and terminals



Biometric Device

CCD / Si Sensor

A/D Converter

CPU / LSI

RAM / Flash Memory

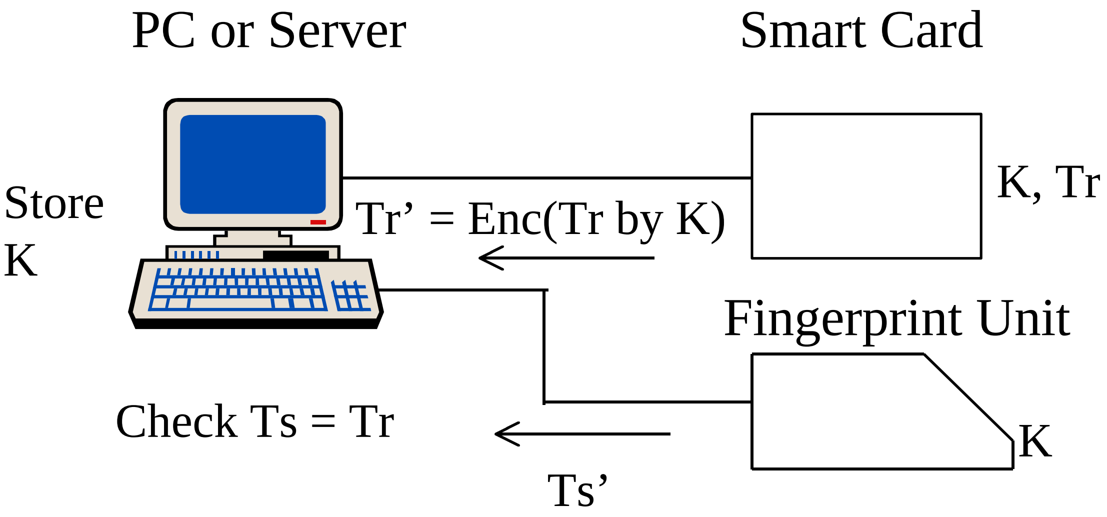
Encypted Serial / USB Port

Host (PC)

Template: On device or host

Application: Authentication provider

2nd generation devices



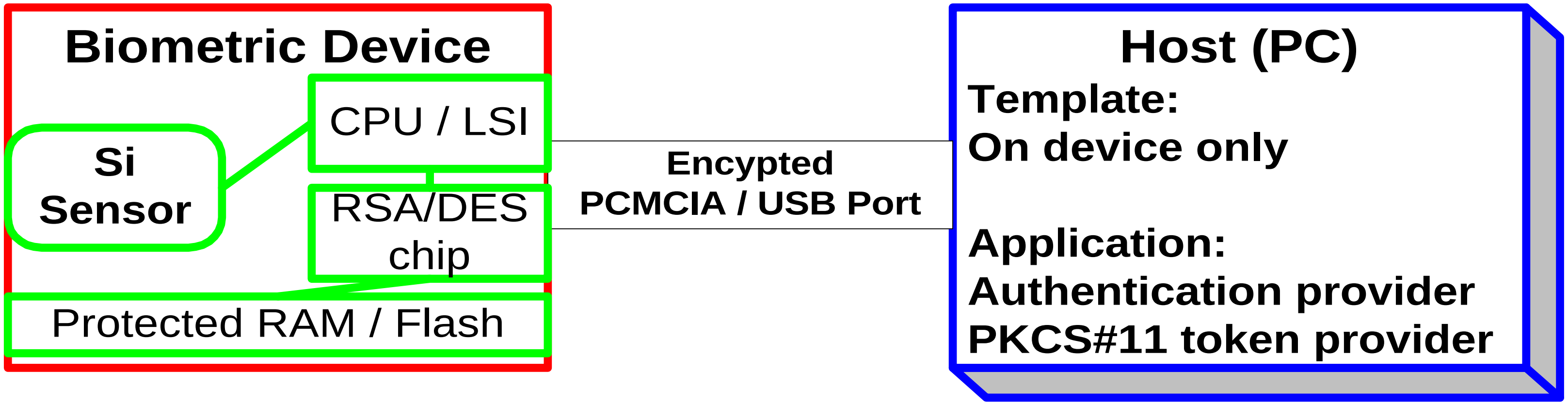
K: Symmetric Key
Tr: Reference Template
Ts: Sample Template

3rd generation devices

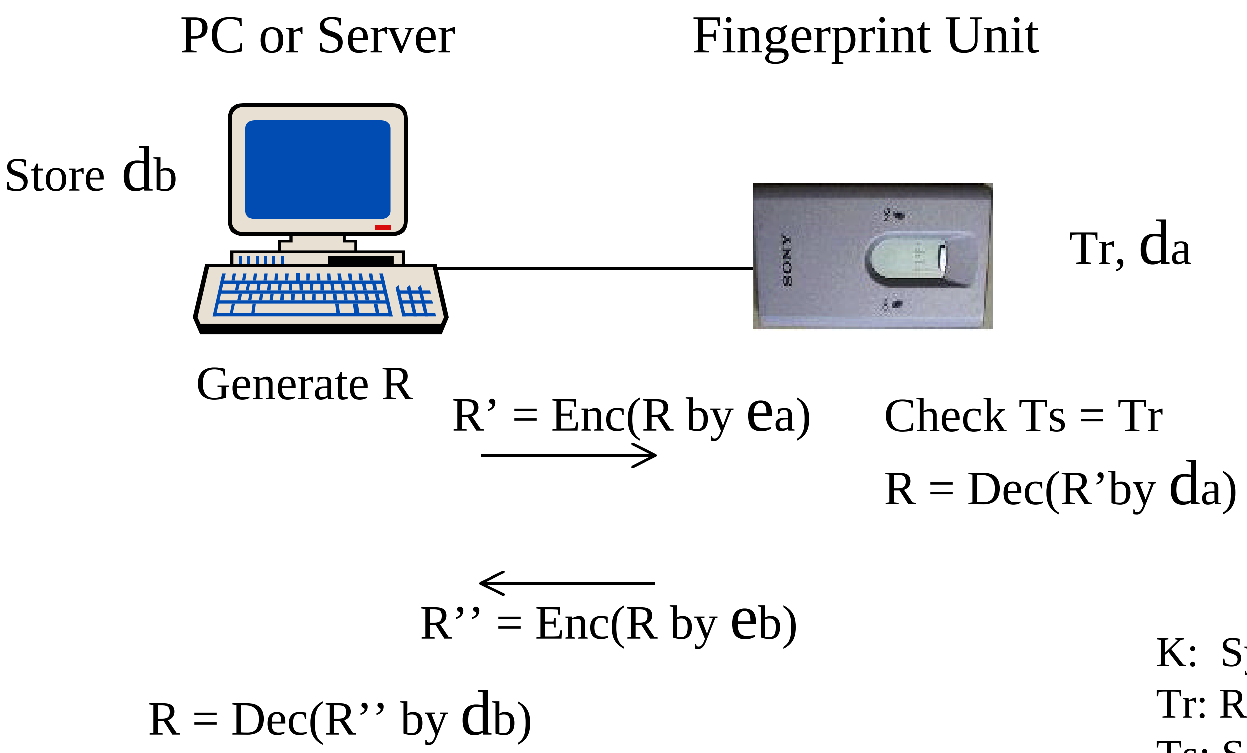
- Third Generation
  - Non optical based sensor
  - First mass produced devices
  - Fast, self-calibrating, encryption support, dead/fake finger detection
  - SDK’s available for PC’s
  - Inexpensive (<$300)
  - Applications:
    - General Purpose Computing
      - Windows NT/95, UNIX

3^{rd} generation devices

- Devices are small and portable
- Templates and private keys (PKI) never leave device (storage is protected)
- Tamperproof (FIPS 140-1)
- Ideal for PKI (PKCS#11 - cryptoki) applications



3rd generation devices



PC or Server

Fingerprint Unit

Store d_b

Tr, d_a

Generate R

R’ = Enc(R by e_a)

Check Ts = Tr

R = Dec(R’by d_a)

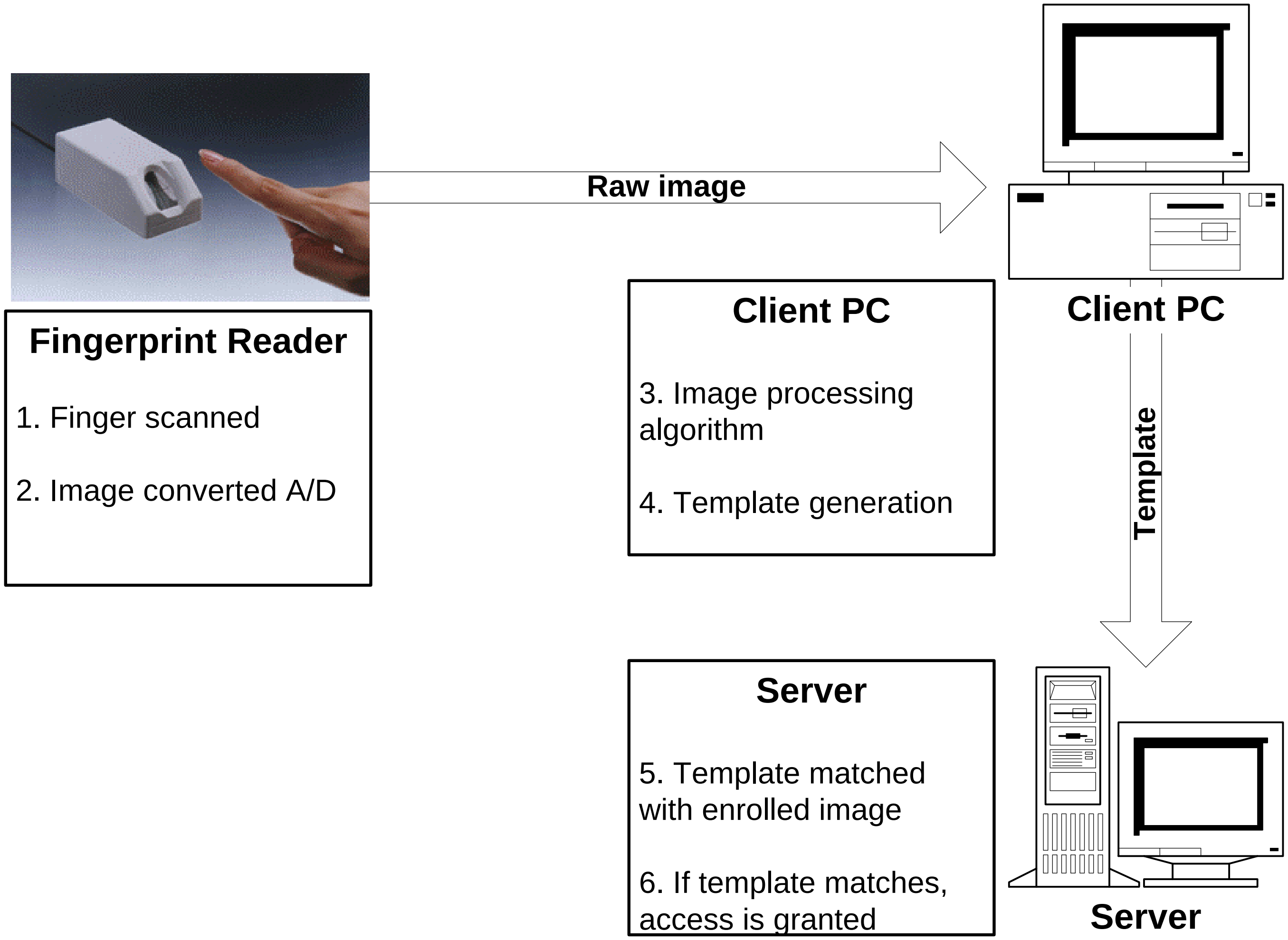
R’’ = Enc(R by e_b)

R = Dec(R’’ by d_b)

K: Symmetric Key
Tr: Reference Template
Ts: Sample Template

Application suitability

Client/Server



Fingerprint Reader

1. Finger scanned

2. Image converted A/D

Client PC

3. Image processing algorithm

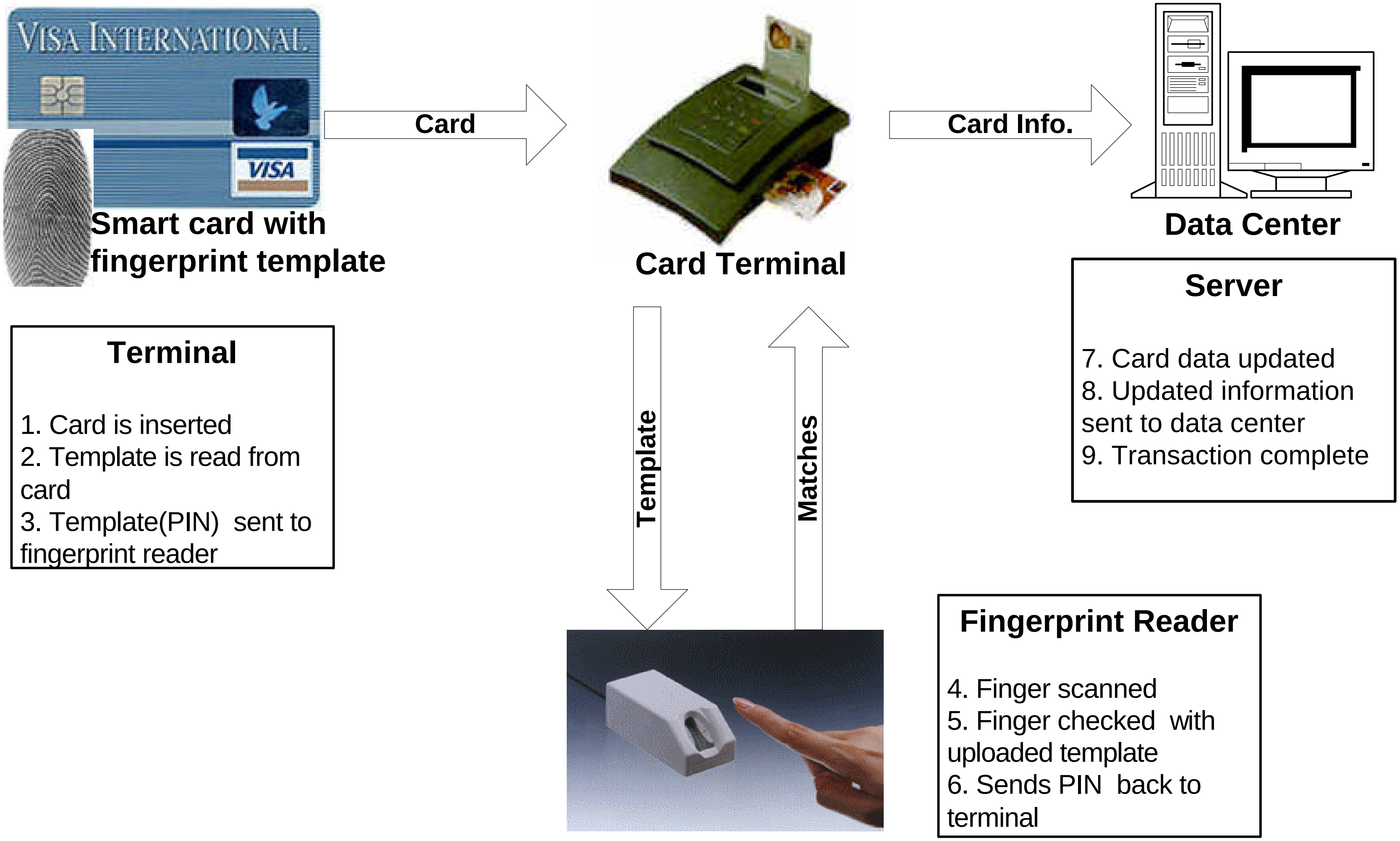
4. Template generation

Server

5. Template matched with enrolled image

6. If template matches, access is granted

Smart card



Smart card with fingerprint template

Card

Card Terminal

Card Info.

Data Center

Template

Matches

Terminal

1. Card is inserted
2. Template is read from card
3. Template(PIN) sent to fingerprint reader

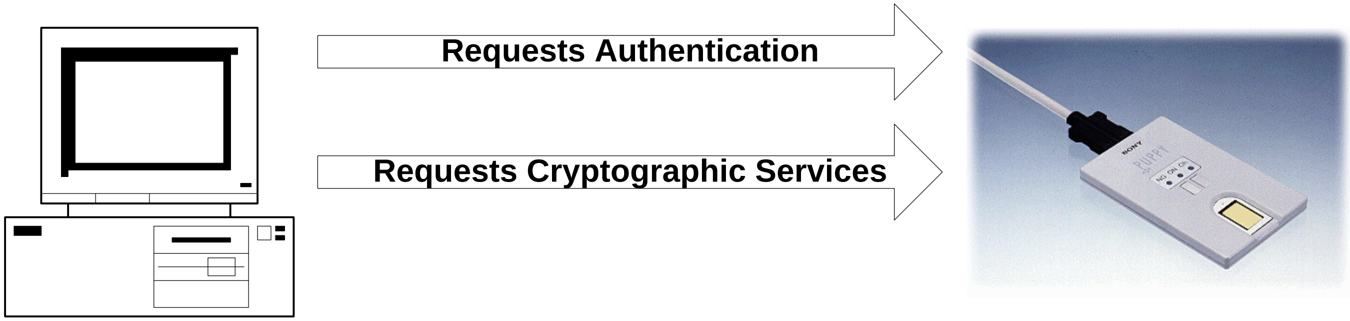
Fingerprint Reader

4. Finger scanned
5. Finger checked with uploaded template
6. Sends PIN back to terminal

Server

7. Card data updated
8. Updated information sent to data center
9. Transaction complete

PKI



Requests Authentication

Requests Cryptographic Services

Workstation

PKI based
fingerprint device

Workstation

Certificate based web site requests certificate
- or -
E-mail application requests private key

PKCS#11 Module

1. User authentication requested

4. Cryptographic services requested -or- certificate requested

Fingerprint Reader

2. Finger scanned
3. Authentication token returned to workstation

5. Cryptographic provided to data -or- certificate returned

Other device features

- Keypads & LED’s
- “Live finger” sensor
- Smart card integration
- Ergonomics
- Size
- Water resistance

Other issues

- FCC, CE, UL certification
- Microsoft WHCL compatibility
- NS1 export approval
- CC1 export approval
- Federal Information Processing Standard
  - FIPS 140-1
- AFIS compatibility

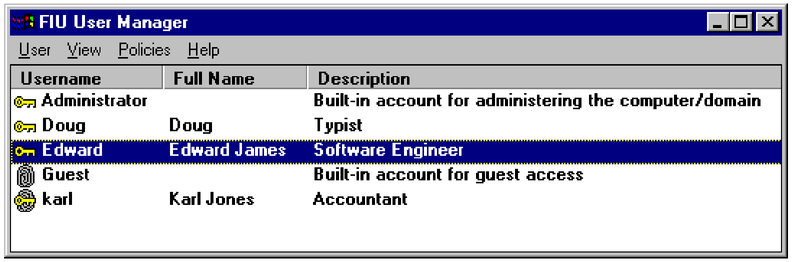
Biometric applications

Types of applications

- Physical access
- Computer logon/logoff
- File encryption
- Client/Server
- Dumb terminals
- Internet / e-Commerce
- Smart cards
- PKI - Public Key Infrastructure

Biometric applications

- SecureSuite
  - Biometrically authenticated Windows 95/98/NT Logon
  - Screen saver unlocking
  - Password provider
  - Hard disk encryption
  - PKI, etc...



Username	Full Name	Description
Administrator		Built-in account for administering the computer/domain
Doug	Doug	Typist
Edward	Edward James	Software Engineer
Guest		Built-in account for guest access
karl	Karl Jones	Accountant

- Smart card (VeriFone)
  - Biometrically locking smart card contents
- Web / Internet Commerce (SecureWeb)

SecureSuite

- SecureStart - Secure logon system for Windows 95/98/NT
- SecureFolder - Windows file / folder encryption application
- SecureSession - Windows password bank / provider
- SecureEntrust - PKI based authentication and encryption provider for Entrust
- SecureApp - Windows based application execution control
- SecureWeb - Customizable web server access control solution

I/O Software, Inc.

Provider of innovative software solutions

1533 Spruce St.
Riverside, CA 92507
(909) 222-7600
(909) 222-7601 FAX
Web: www.iosoftware.com
E-Mail: William@iosoftware.com

I/O Software - World Headquarters -