IDENTITY-AS-A-SERVICE IN A MOBILE WORLD

Cloud Management of Multi-Modal Biometrics

IWS® IMAGEWARE® SYSTEMS, INC.

ImageWare® Systems, Inc.

- Headquarters in San Diego, CA
- Offices worldwide (US, Canada, Germany, Mexico)
- Over 15 years of experience in biometric identity management, law enforcement, border control, airport security, biometric smart-cards, military, intelligence, and more…

David Harding
Chief Technology Officer & Vice President
dharding@iwsinc.com

IWS Has Been the Pioneering Force and Established Innovator

in biometric security for over 15 years, with a strong installed-base, providing advanced solutions to:

- San Bernardino County Sheriff' s Department
- U.S. Department of Veteran Affairs
- Country of Mexico[1]
- LAX – Los Angeles World Airports
- Arizona Department of Public Safety
- Canadian Air Transport Security Authority
- New South Wales Police (Australia)

[1] Indirect via a prime contractor partnership

Wired Magazine Recently Ran the Headline....

"KILL THE PASSWORD: WHY A STRING OF CHARACTERS CAN'T PROTECT US ANYMORE"

MOBILE DEVICES ARE EVER-PRESENT AND ARE REPLACING THE PC

"Almost 40% of Americans used smart mobile devices for banking and purchases"

– Source: Federal Reserve 2012

"Android devices are expected to almost triple over 5 years, while iOS could grow about 140%"

– Source: Gartner Group 2013

SECURITY REMAINS THE BIGGEST CONCERN

“Among consumers who do not use mobile financial services, the principal reasons cited for not using the services are perceptions of limited usefulness and benefits, and **concerns about security.**”

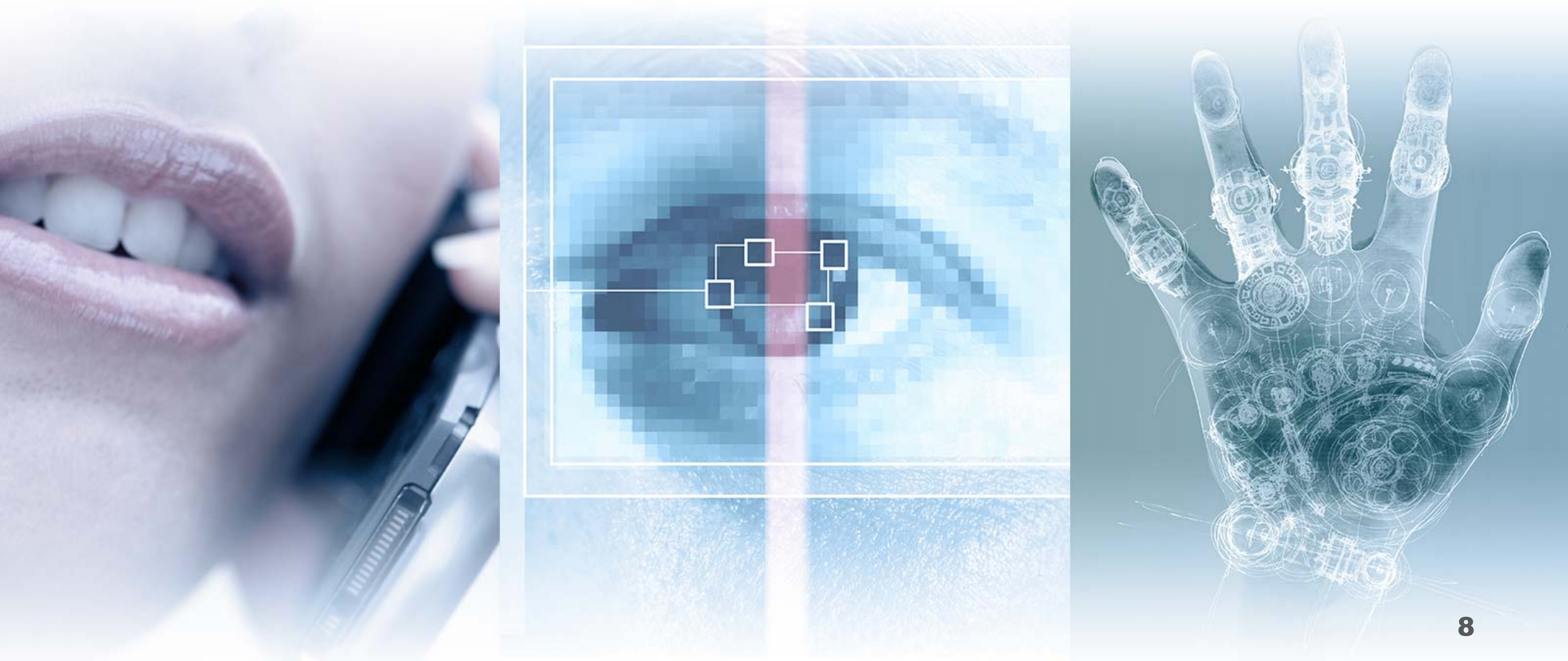
– *Source: U.S. Federal Reserve Bank 2014*

Cloud Computing and The Pervasive Growth of Smart, Mobile Devices

has made secure identity authentication an absolute necessity.

And an essential reality.

THAT REALITY IS MULTI-MODAL BIOMETRICS.



MULTI-MODAL BIOMETRICS UNITES MULTIPLE BIOLOGICAL TRAITS TO SECURELY CONFIRM AN IDENTITY

Voice

Finger Veins

Palm

Face

Signature

DNA

Behavioral

Fingerprint

Retina

Hand Geometry

Iris

MULTI-MODAL BIOMETRICS OFFERS A GREATER LEVEL OF SECURITY

Single-modal biometrics, historically and effectively, have serviced a defined and limited-size populous and situation.

Multi-modal biometrics can be used together and/or singularly based on the situation and environment.

THE U.S. GOVERNMENT CONFIRMED MULTI-MODAL BIOMETRIC IDENTITY MANAGEMENT AS THE *ONLY* WAY TO MOVE FORWARD.

FBI, Dept. of Defense, Law Enforcement, International Civil Aviation Organization, Homeland Security Presidential Directives 5 & 12

Multi-Modal Biometrics Will Become as Ubiquitous as Smartphones

Mobile devices are the perfect biometric capture device.

We have them with us.

They give us access to services and data anywhere anytime.

Issues to Mobile Biometric Adoption

- Match-on-Device vs. Match-in-Cloud
- Scalability
- Reliability
- Security
- Modality Selection
- Maximizing Identity Verification Services
- Ease of Use

Match-on-Device

Susceptible to:

- Theft of biometric enrollment
- Replacement of biometric enrollment
- Reverse engineering of biometric template (“hill-climbing attack”)

Does not support:

- Enroll once, use on many applications and devices
- Duplicity check for enrollment verification
- Transfer of biometrics to new devices and/or applications

Does not scale and is not trusted!

Match-in-Cloud

- Single, secure biometric enrollments for each modality
- Single, trusted source for biometric identity verification
- Device independent – enroll once, use on any device
- Service and application independent
- Use the right biometric for the situation and environment
- Use multiple biometrics for “high-confidence” required transactions and to prevent “*spoofing*”

What's Needed to Make it Work?

A real-time, high performance, highly scalable, multi-modal, biometric database

Must support today's technology as well as tomorrow's

Must scale to support large populations

Must support *anonymous verification*

GoCloudID™ – The Scalable, Cloud-based, Biometric, Identity Management Platform

- Reliably manages access to biometric enrollment & verification
- Can be used as an end-to-end or modular solution
- Offers full and anonymous identity management
- Conveniently enables applications on all mobile devices
- Deployment is rapidly integrated, flexible & scalable
- Operates as a multi-tenant system
- Web portal is customer/partner provisioning
- No start-up costs
- Pay-as-you-go and scale-as-you-need

GoCloudID™

The Only Multi-Modal CloudID SaaS/PaaS License and/or Subscription Service Today

IWS’s Patented Biometric Engine® 2.0,

the backend database of GoCloudID, delivers revolutionary capabilities

- Enrollment, identity & verification management of unlimited population sizes
- Hardware & algorithm independent processing
- Compatibility with all biometric products
- Future-proof, plug-n-play flexibility
- Full and anonymous biometric identity verification
- Software development kits

IWS® Biometric Engine®

License and/or subscription service offering as part of GoCloudID™

IWS’ s Patented GoMobile Interactive™

The Cloud-Based, Interactive, Push Messaging Server for Mobile

- Pushes *interactive* messages to mobile devices
- Customized message workflows and integrated biometric identity authentication
- Software development kits for rapid integration
  - Server
  - Mobile applications
- Enables in and out-of-band identity authentication

GoMobile interactive

License and/or subscription service offering as part of GoCloudID™

Making it Work in the Real World / Example - Out-of-Band Authentication

Out-of-Band Authentication uses a mobile device to verify the identity of someone who is attempting to access data or services

Biometrically enables:

- Website logins
- HTML5 mobile applications
- Mobile wallet and credit card transactions
- Loan applications
- Anytime you need to verify an identity

Steps to Biometric Verification Using a Mobile Device using Out-of-Band

Three factors:

- What you have
- What you know
- Who you are

Steps to out-of-band identity verification:

- Invoke the device (push message)
- Capture credential(s) and/or biometric(s)
- Verify the identity in the cloud and notify the service

IWS’ s GoVerifyID Mobile Application

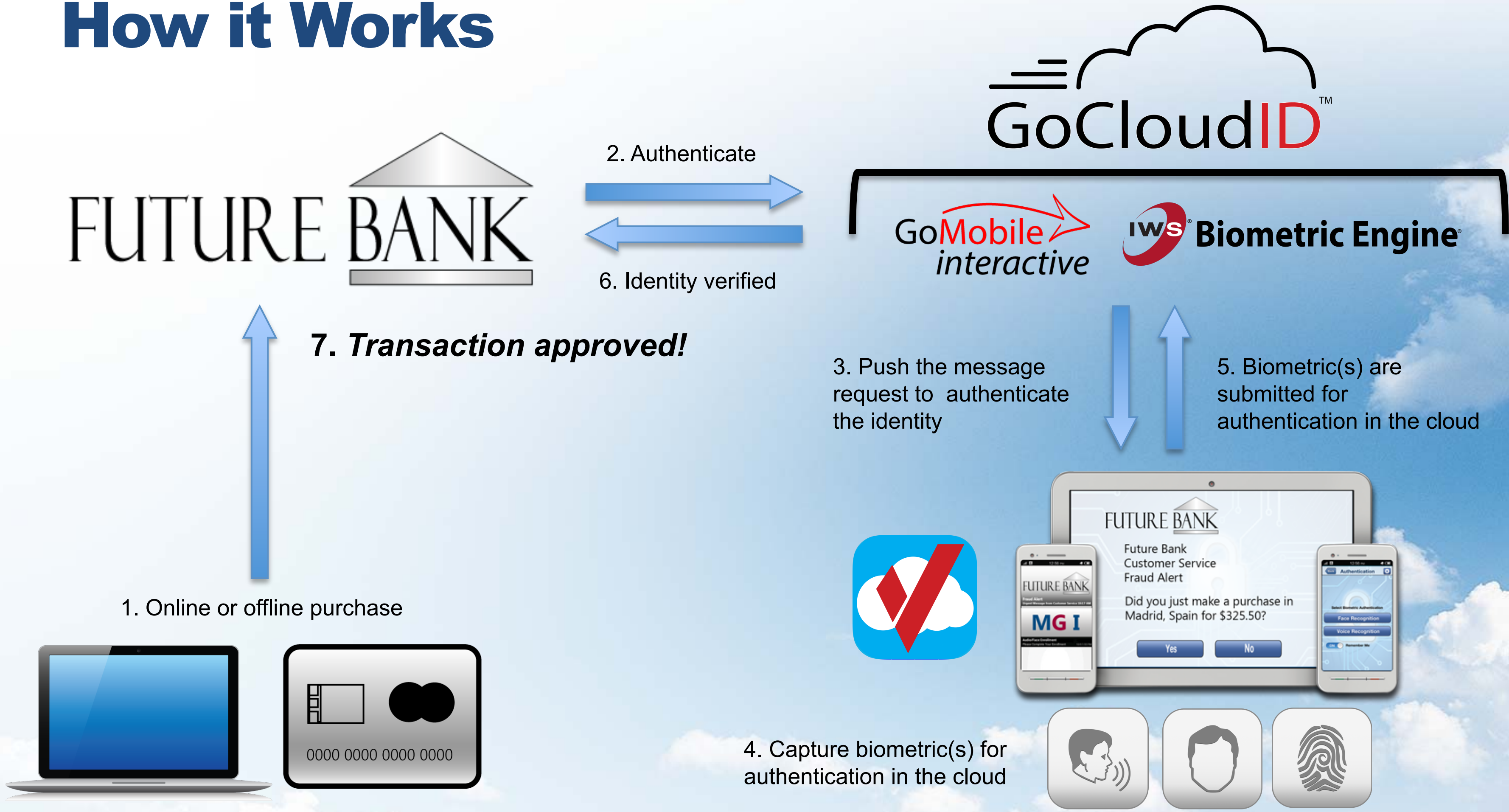
Turn-key, Out-Of-Band Authentication Using a Mobile Device

- Mobile application for iOS and Android devices
- Receives authentication push messages from *GoMobile Interactive*
- Collects requested biometric(s) and securely sends them to the cloud for identity authentication (GoCloudID)
- *No mobile application coding required*

GoVerifyID™

License and/or subscription service offering as part of GoCloudID™

How it Works



1. Online or offline purchase

2. Authenticate

3. Push the message request to authenticate the identity

4. Capture biometric(s) for authentication in the cloud

5. Biometric(s) are submitted for authentication in the cloud

6. Identity verified

7. *Transaction approved!*

Future Bank
Customer Service
Fraud Alert

Did you just make a purchase in Madrid, Spain for $325.50?

Example 2: pillphone® transforms medication compliance with mobile technologies & patient engagement

patient
caregiver
pillphone
Katherine Williams
My Meds
Pill Lookup
Reminders
Messages
Dosage Diary
Caregiver
provider
pharmacy

pillphone® is an Enterprise level FDA cleared mobile communication platform that:

- **Connects** patient with healthcare providers
- **Promotes** interactive communication
- **Ensures** medical compliance with personalized reminders
- **Integrates** with medical supply chains
- **Empowers** disease management and wellness education

It's secured with multi-modal biometric enabled identity management and interactive push messaging to ensure patient verification.

HIPAA compliance

FDA Cleared

THE TREND IS IN MOTION.

The future of identity authentication is multi-modal biometrics.

Using Cloud and SaaS, adding scalable, biometric identity management and out-of-band authentication to mobile applications has never been easier or more cost effective.

IWS® ImageWare® Systems, Inc.

SECURING YOUR FUTURE