

AT&T Developer Program – devCentral Webcast Series

Biometrics in Enterprise Security

Presented by:

Lai Lau
Senior Manager
AT&T Enterprise Developer Program

Art Maria, CISSP
BMG SE&A Chief Enterprise Architect
AT&T Mobility

Andy Germano
Director of Wireless Markets
AuthenTec

Rod Beatson
President
Transaction Security, Inc.



Introduction – AT&T Network Advantage

Wireless Network Coverage - America's largest digital voice and data network and the broadest international coverage of any U.S. carrier

- Voice - 6 continents and over 190 countries
- Data – Over 130 countries with 3G in over 40 countries
- Unlimited calling within the largest mobile-to-mobile calling community—over 62 million people and growing.
- 3G on the global standard - UMTS/HSDPA in over 165 major metro areas and growing.

Business Focus and Expertise

- Serving all Fortune 1000 and Standard and Poor's (S&P) 500 companies
- Wireless Data Leadership - cutting-edge data products and services – the leader in wireless corporate e-mail
- Ecosystem of trusted market leaders and rich experience with deployments in multiple industries

Art Maria, CISSP

BMG SE&A Chief Enterprise Architect
Business Markets Group
AT&T Mobility

Biometrics

Introduction

What are biometrics?

Biometrics versus the alternatives

Types of biometrics

How biometrics work

- Finger print
- Iris
- Face
- Voice
- Signature/Sign

Cultural and Social Issues

Comparison

Conclusions

The Vulnerability of Mobile Devices

25 million people will need a new cell phone this year because theirs has been lost or stolen. – *MSNBC, February 5, 2007*

Theft of mobile phones is costing U.K. consumers 390 million pounds every year, with one phone stolen every 12 seconds. Thieves are even snatching phones from victims' hands as they walk down the street. – *Halifax Home Insurance, May 18, 2006*

"...nearly one in four have had their PDA lost or stolen." – *Palm Info Center, May 3, 2004.*

Over 40% of people have lost a mobile phone and a staggering quarter have lost a laptop or PDA or both. – *PDA Usage Survey 2003*

Over 7 million cell phones were reported lost in South Korea between 2000 and June 2002. – *The Financial News, August 26, 2002*

In Amsterdam, mobile-phone theft rose by 80% in 2001; in the U.K., it jumped almost 200% from 1995-2000. – *Time, March 11, 2002*

Results of Enterprise Study*

75% indicate extending business applications to mobile workers is becoming more of a priority.

63% view extending paper-based and desktop applications to handheld devices as ***critical*** for maintaining the competitive advantage of their businesses.

Applications targeted in the next 12-months.

- Intranet access
- CRM
- Inventory management
- ERP

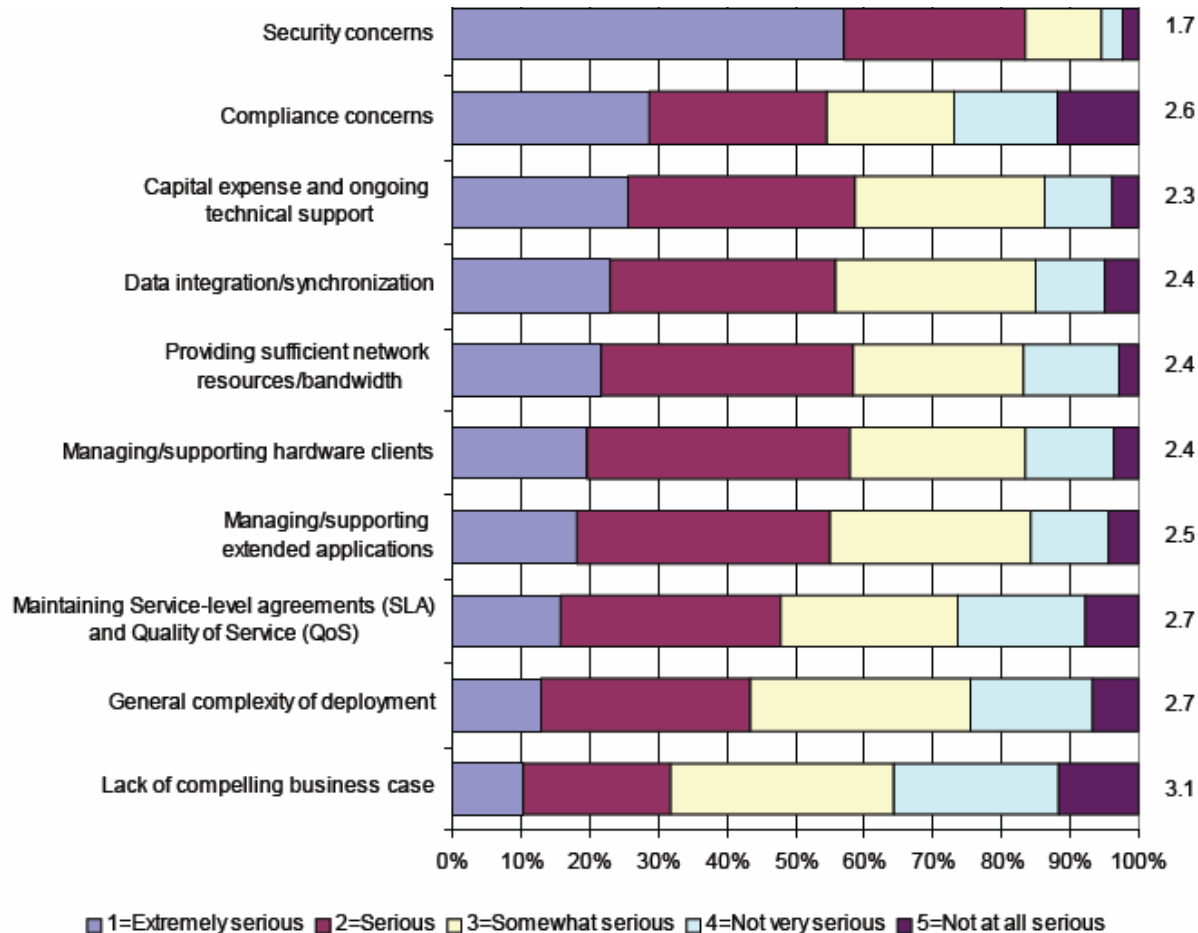
Justifying the acquisition requires demonstrating the potential for:

- Increasing productivity (80% significant factor) and
- reducing costs (65% significant factor)

* TechRepublic Feb. 2006. 375 cross industry respondents, North America

Security is #1 Concern (by far)

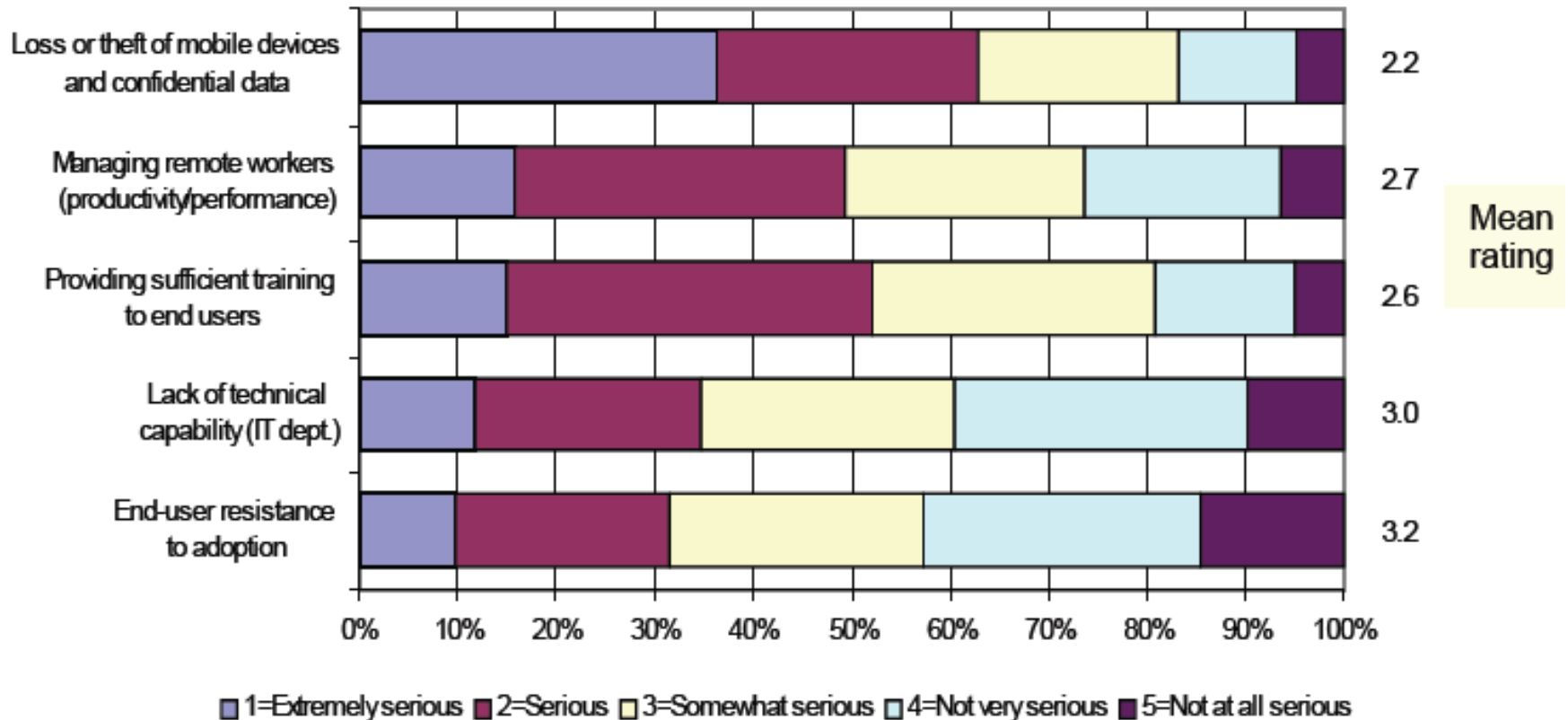
Please rate the significance of the following technical problems to mobile data and application deployment for your organization



Over 95% of CIO's rated Security as Serious Concern

Loss or theft of devices = #1 issue

Please rate the significance of the following personnel issues sometimes associated with mobile data and application deployment for your organization.



A Real World Example

The Transport for London's Lost Property Office



Around **15,000** mobile phones and PDAs are handed in to *Transport for London's* lost property office each year.

The lost property office keeps items for three months and then has to get rid of them to make space for newly lost phones being handed in.

What are Biometrics

Biometrics are:

- Measurable
- Physiological and/or behavioral characteristics
- Can be used to verify the identity of an individual

Biometrics Versus Other Authentication Mechanisms

What you know: User name, password, pin

What you have: Tokens and smartcards

Who you are: Biometrics

Details on biometric technologies

Why biometrics

Only biometrics can verify *you* as *you*

Biometrics are unique among authentication schemes in that they cannot be:

- *Lost*
- *Stolen**
- *Duplicated*
- *Forgotten*
- *Observed*
- *Broken**
- *Written down*

Password and/or Token does not assure that you are who you claim to be

*Some exceptions will be noted later.

Types of Biometrics

Physiological

- Fingerprint*
- Iris*
- Hand (including knuckle, palm, vascular)
- Face*
- Voice*
- Retina
- DNA
- Other Odor, Earlobe, Sweat pore, Lips

Behavioral

- Signature/Sign*
- Keystroke
- Voice*
- Gait

*Biometrics most applicable to mobile devices

How Biometrics Work

During enrollment, the user provides multiple samples of the relevant biometric to the system, these are converted to digital or other representations and stored

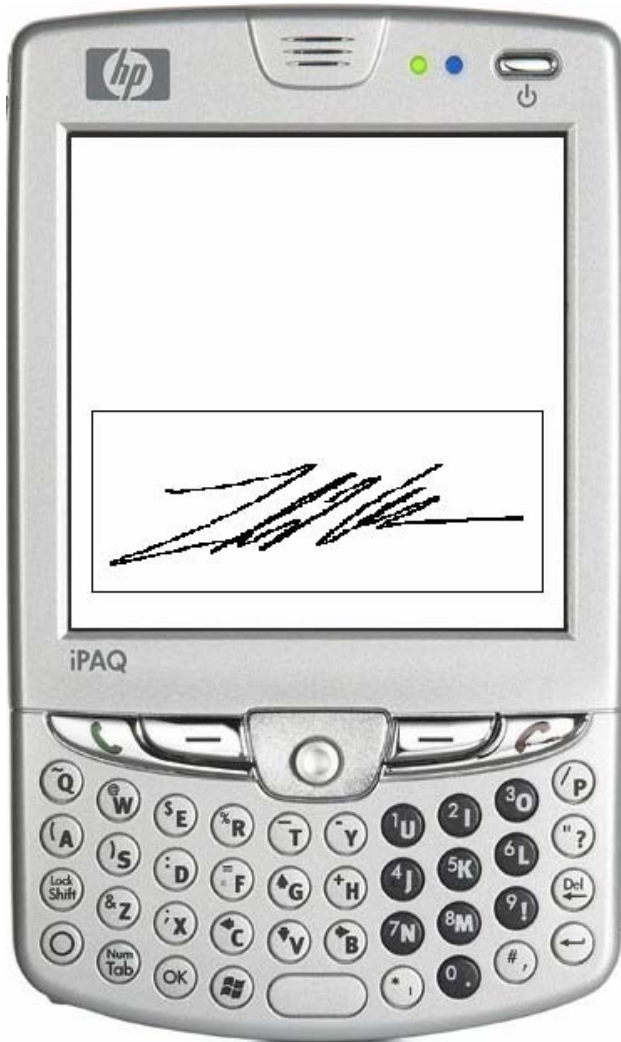
Once enrolled the user can use the biometric system. Biometric access is called a live scan

A live scan can be used two ways:

- For identification, to identify a user from the pool of enrolled users
- For authentication, to confirm a user is who he/she claims to be.
Used in conjunction with a user name, pin, password, or token

Most biometric systems use each successive live scan to improve the template

Signature/Sign Recognition



- Requires only a stylus, a touch screen digitizer, and software; perfect for PDAs
- Sign name, write word, or draw secret sign 3 to 10 times to enroll
- Signature/Sign is captured and (if necessary) stored as a vector representation rather than a bit mapped image.
- The Vector uses speed, direction, pen lifts, turning points and possibly pressure to create the template.

Signature/Sign Recognition

- No one signs exactly the same way twice in a row, so identical matches are automatically rejected and this prevents playback of the template data as a sample.
- Highly reliable and easy to deploy
- Some, but not all, vector signature systems are subject to attack by calculating the signer's secret keys from some triplets of messages, signatures and error patterns.
- Available today for PDAs and Tablet PCs

Cultural & Social Issues

Social Constraints

- Health
 - Some people have a concern for the physical effects of the technology upon them.
 - This accounts for the greater acceptance of newer iris recognition technology over the older retinal scan technology.
- Religious and Cultural
 - Certain cultures and religions prohibit or look with great disfavor upon photographing of individuals making facial recognition unacceptable.
- Privacy
 - Some individual may object to supplying certain biometric samples such as voice or finger print
 - Technologies such as facial or signatures recognition may be more acceptable

Comparison of Biometric Technologies

Characteristic	Password	Card or "Token"	Finger Print	Iris	Facial	Voice	Signature
Low or no additional hardware costs	Yes	No	Varies	Yes	Yes	Yes	Yes
Versatile hardware (used for other purposes)	Yes	No	Yes	Yes	Yes	Yes	Yes
Multiple hardware vendors	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hard to crack	No	Yes	Varies	Yes	Varies	Varies	Yes
Can't be lost or stolen	No	No	Varies	Yes	Yes	Yes	Yes
Can't be forgotten	No	No	Yes	Yes	Yes	Yes	Yes
Can't be copied	No	Varies	Varies	Yes	Varies	No	Yes
User-friendly	No	No	Yes	Yes	Yes	Yes	Yes
Currently available for mobile devices	Yes	Yes	Yes	No	No	Yes	Yes

Conclusions

Biometrics offer superior security, excellent usability, and moderate cost as compared with other authentication technologies

Of the biometric technologies currently available on mobile devices, vector signature stands out for its ease of use, low cost, and high security

Of the biometric technologies in development for mobile devices, only iris recognition compares to vector signature

Enterprises are encouraged to add biometrics through third party solutions.



From Transaction Security

Rod Beatson

President, Transaction Security, Inc.
919-372-1849

Device Access Security at the Perimeter Is Vital

Device Data can be Very Private & Highly Confidential

- Mobile Devices Migrating to Lap Top Functionality
- Confidential Emails
- Calendar & Contact Information
- Corporate Documents From VPN
- Personal Information
 - Credit Card/Bank accounts
- Passwords

Devices Provide Network Access

Devices Very Susceptible to Loss or Theft.

- Make Them More Secure than Laptops

Device Access Security at the Perimeter Is Vital

An Impostor Blocked at the Device Implies an Impostor Blocked from the Network

But:

- Virtually All Access To Devices & Networks Currently Rely on Passwords
- The Password might be:
 - Known by an Impostor
 - Guessed by an Impostor
 - Passed on to an Impostor

In Which Case:

- The Device and the Network are Compromised with 100% Certainty.

Passwords: Unfriendly & Insecure

Password Entry:

- 8 character (or Greater) mixture of Upper Case, Lower Case, Numeric & Special characters – Ouch!!

Remember the Password Please

- Even When it keeps changing – Ouch!
- A Large % Of Help Desk Costs are Password Related

Password Rules Tend to be Relaxed to deal with the Unfriendliness.

- Which makes them even less secure – and still Unfriendly



Using The Crypto-Sign SDK Signature/Sign Biometric Technology



- SDK Information From Info@crypto-sign.com
- Secret Sign Biometric Algorithms Developed Over Several Years
- Remote Enroll, Verify, Identify
- First PDA Access Control App. Beta-Tested By Microsoft and Others
- SDK Developed For General Use
- First Mobile Enterprise App.
 - #1 Global Medical Device Manufacturer



Use Scenarios For The Crypto-Sign SDK Signature/Sign Biometric Technology



- User Authentication for Device/Application Access Control
- Key Generation/File Encryption
- Network Access/Mobile VPN
- Electronic Signatures
 - With an Ink-on-Paper Look
- On-Line Banking
- Payment Systems/M-Commerce



Secret Sign Example

Mobile Device User Authentication

Password Release

- Submit **Secret Sign** on Power-Up Screen
- **Inking Inhibited** To Preserve Privacy
- Secure User Friendly Authentication
- **No Need To Remember/Enter Password**





Secret Sign Example

Mobile Device User Authentication

Password Release

- Submit **Secret Sign** on Power-Up Screen
- **Inking Inhibited** To Preserve Privacy
- Secure User Friendly Authentication
- **No Need To Remember/Enter Password**





Secret Sign Example

Mobile Device User Authentication

FOR EXTRA SECURITY (If Required)

- Enter PIN
 - Device Access
 - Network Access
 - High Value Transactions
 - Confidential Files

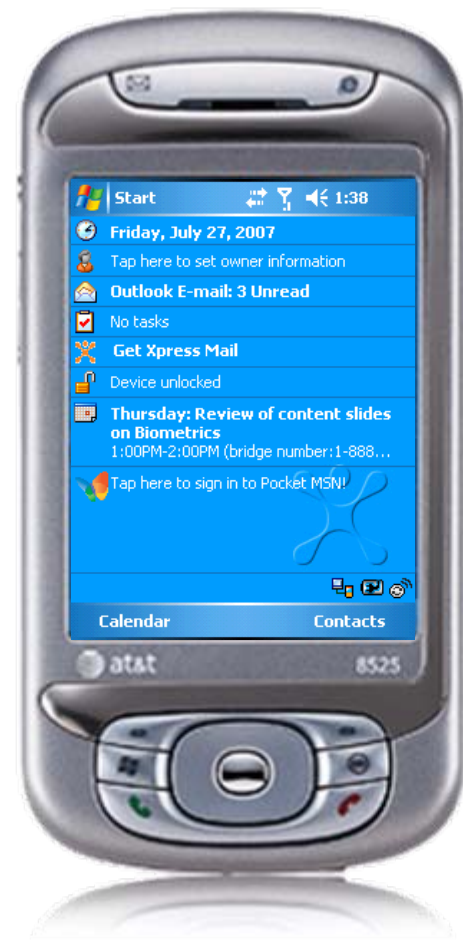




Secret Sign Example

Mobile Device User Authentication

- Successful Biometric Match/PIN Gains Access
- Software-Based, Simple, Low Cost, User Friendly
- PIN/Biometric Sample Combination can not be Defeated by Impostor





Capture Sign On Device

Match Sign On Device & Server

- **Belt & Suspenders**

- Can Add to User/Device/Server Trust

- Use:

- ANSI/INCITS 358 – The BioAPI Specification

- ANSI/INCITS 395 – Signature/Sign Biometric Data Interchange Formats

- **These and Other Biometric Standards are available from ANSI**



Biometrics:- A Better Way

Biometric Access Control – With PIN

- Submit Biometric Sample
- Client Extracts Features using the Crypto-Sign DLL
- Enter PIN
- Client Generates Encryption Keys Using
 - PIN Hash, Stored Encrypted Password & Hardware Components
- Client Decrypts Template
- Client Matches Sample to Template

Good Match?

Yes → Decrypt & Release Stored Password, Update & Re-Encrypt Template.



Biometrics:- A Better Way

Biometric Access Control – with PIN

- Wrong PIN → Template Does not Decrypt
- Bad Sample → No Biometric Match

Both PIN and Sample Must be Good

- Probability of Impostor submitting correct combination is $< 1/1,000,000$
- FIPS 140/2 Level 3 Authentication Requirement

Unlike Passwords this is Not Susceptible to Brute Force Attacks



Biometrics:- A Better Way

Biometric Samples can not be easily Guessed, Spoofed or Passed on.

- Inhibit Display of Submitted Sample
- Delete Sample Data from Client after Extracting Features
- Delete Feature Values from Client after Matching against Template
 - No Playback Possibilities

Good Match of Biometric Sample Against Template (Plus PIN for Greater Security) Releases Password.

- Password Released by Client Software
 - No Need to Enter or Remember it !!!!

Can still Use Existing Password Authentication Protocols for Network Access and Transport Layer Encryption



Biometrics:- A Better Way

Need Encryption & Biometrics Working Together

- Encrypt Biometric Template & Password on Device Client.

Generate (Don't Store) Encryption Keys on Client Using one-way PIN Hash Plus Device Specific Hardware & Other Information

- Encrypt/Decrypt Biometric Template
- Encrypt/Decrypt Password
- Other Designated Sensitive Data
- Specific File Encryption



Secret Sign Example For Proof of Authorship

Electronic Signature Release

- Submit **Secret Sign** in Signature box
- **Inking Inhibited** To Preserve Privacy
- Secure User Friendly Authentication





Secret Sign Example For Proof of Authorship

Electronic Signature Release

- Submit **Secret Sign** in application box
- **Inking Inhibited** To Preserve Privacy
- Secure User Friendly Authentication



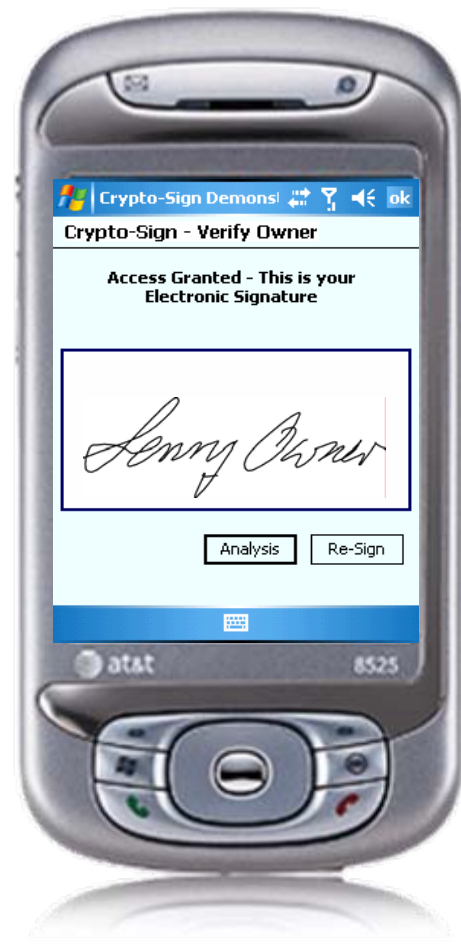


Crypto-Sign®

For Document Integrity

Proof Of Authorship - Secret Sign Releases Electronic Signature

- Fast, Low Cost, User Friendly
- Sandia Laboratories Tested Algorithms
- Remote Electronic Signing
- Document Security
- Healthcare/Financial/Legal Applications
- Government Applications





Access Control Using Crypto-Sign

A Signature/Sign Biometric Technology

Uses A Handwritten Secret Sign Submitted on the Device Screen with a Stylus

- Impostor Has no Idea what Sign to Submit
- Timing & Spatial Features both Important
- Cannot be Spoofed
- Even if the Impostor knows what it looks like.

Users are in Total Control of the Biometric Sample

- Can Change the Sign at Anytime
- Just just like a PIN or Password

In Control of their Own Privacy & Security



Further Information From:

- The Crypto-Sign Web Site At:
<http://www.crypto-sign.com>
- For Information on TSI's SDK
info@crypto-sign.com
- VideoClips of Microsoft's Mobility Marketing Manager & Rod Beatson, TSI's CEO on The Importance of Mobile Device Security
http://www.crypto-sign.com/dedo_beatson_video.php
- A Crypto-Sign White Paper At:
<http://www.crypto-sign.com/CryptoSignWhitePaper.pdf>
- Information on TSI At:
http://www.crypto-sign.com/about_tsi.php

Thank you!