# G/J TDC Presentation Narrative

# *1 G/J TDC Presentation*

= = = This is the start of COMPANY OVERVIEW

# (General Presentation)

# Company overview

## 2 Goldhar/Jaffe Technology Development Corporation

(show logo)
Was created in 1997 to develop intellectual property, initially the patented concept of indigenous authentication for sensor-recorders and other information capture devices.

## 3 Jonathan E. Jaffe, CPA, MS

(show picture)
Entrepreneur with five currently operating businesses
Developed four pieces of software for military and public use
Lead developer for Signa2

## 4 Joel D. Goldhar, DBA

(show picture)

Former Dean of the Stuart School and current Professor of Operations and Technology Management at the Illinois Institute of Technology Dr. Goldhar is a graduate of RPI, Harvard Business School and George Washington University.

At the National Academy of Engineering / National Research Council he was Executive Director of the Manufacturing Studies board. He has served Executive Secretary of the Committee on Computer Aided Manufacturing and The Committee on Computational Mechanics as well as Program Director for User Support Studies and The Economics of Information at the National Science Foundation.

At the National Academy of Engineering / National Research Council he was Executive Director of the Manufacturing Studies Board, Executive Secretary of the Committee on Computer Aided Manufacturing and Executive Secretary of The Committee on Computational Mechanics. At the National Science Foundation he was Program Director for User Support Studies and The Economics of Information in the Office of Science Information Services.

= = = This is the end of COMPANY OVERVIEW

= = = This is the start of THE PROBLEM

# WHAT IS THE PROBLEM?

## 5 Why is Authentication Important?

(pre digital) Forgery, fraud
Authentication is necessary for commerce, industry, cornerstone of binding agreements.
Ronald Reagan said “Trust but verify”.

## 6 Why is Digital Authentication Important?

General move from paper to electronic does not remove need for authentic documents and it is so easy to alter digital files.

## 7 The Problem Defined Via Examples

## 8 3rd eye in head

If you received a digital photograph of a person with a third eye in the middle of their forehead, you would likely suspect it had been altered.

## 9 Her Eyes / Blue

Would you be as quick to identify a change from blue eyes to brown eyes?

## 10 Her Eyes / Green

Or are they green?

## 11 Her Eyes / Which? (shows both)

Were they originally green or blue?

## 12 Has this check routing number been changed?

(check with changed routing number)

## 13 Hajj/AP smoke

Obvious alteration but human editors missed it

## 14 1984 Olympics / Mary Decker Slaney (as printed)

1984 Olympics. Mary Decker Slaney falls after being tripped by Zola Budd. The image was printed over two pages. The vertical crease is the paper fold. Other than being cropped is the image authentic?

## 15 1984 Olympics / Mary Decker Slaney (Original)

In addition to being cropped the original image was brightened to remove shadows from the runner's face. The antenna from the radio in the assistant's left hand was removed from the runner's chin. Here is an excellent pre-digital alteration and human editors missed it. Does it really matter? Sometimes no, sometimes yes.

## 16 Liver – Altered

CT Scan of a 66 year old female showing a large metastasis in the central area making for a doubtful surgical outcome.

## 17 Liver – Original

Here is the original image. Several small metastases had been removed, but most significant change was moving the large metastasis from the right posterior lobe toward the anterior. These images appeared in the <emphasis> 1995 </emphasis> American Journal of Radiology as an example of possible alterations. Why would someone want to alter an MRI or any medical document?

## 18 Fake Jimmy Carter

In 1989 John and Tom Knoll created Photoshop and never anticipated how it would be abused to change digital files in a manner hard or impossible to detect.

## 19 Fake-check_routing_number

Where file validity is legally or financially important, this challenge to using digital files presents a major impediment to broader adoption; despite the otherwise compelling cost and ease-of-use advantages of digital technology.

## 20 Fake-eye-blue

Digital fakery is widespread and becoming increasingly sophisticated. The ease of use, low cost and wide availability of programs like Adobe's Photoshop or PaintShopPro gives anyone the capability.

## 21 Fake-eye-green

The October 2005 issue of Popular Science had a particularly good article on this topic. A Google search on the topic yields many relevant articles and reports. (her eyes were actually brown)

## 22 Fake-Liver-altered

In 2009 no digital image can be truly trusted. Paper images can also be scanned, altered and reprinted. Many digital files can also be altered and reproduced without detection.

## 23 Our Market Space

(slide showing the below words)
Our market space is any situation in which there is a reason to distrust the information source; or a need to have a very high confidence in the source veracity.

## Major trends

24 Altering digital files will get easier.
Altering digital files will continue to easier and more elegant. This is the general trend of software development, more features, more power, easier to use.

25 Public and institutional skepticism will increase
There will be a growing lack of trust in both digital images/files/sources in and from the institutions of authority.

26 Regulations and legal precedents will require longer term storage of documents including transaction data

27 Despite the above there will continue to be a movement to fully digital storage.
Therefore the world needs and will eventually demand a user friendly, consistent and robust way to identify 'trusted' digital images, documents and files. There are two reasons for this. One is cost. The other is true survivability requires multiple backups and geographically diverse locations. This is more practical with digital files.

## A Question of Logic

### 28 A Question of Logic – Mona Lisa

(picture of the Mona Lisa-50)
Who was the best art forger of all time?
**<PAUSE - SLOW SPEECH SPEED>**
We don't know because his, or her, work isn't known to be a forgery. Maybe Mona knows the artist wasn't Da Vinci but she isn't telling, only the smile survives.

### 29 A Question of Logic – None Discovered

(Mary Decker Slaney altered image, liver altered image)
"No alterations were discovered."
This is the best that can be said about an image. Logically you cannot state it is unaltered. That is attempting to prove a negative. The best you can say is that "no alterations were discovered."

### 30 A Question of Logic – Image Unchanged

(Mary Decker Slaney original image)
"This image is unchanged."
This is a *positive affirmation* of originality. It is possible because the Signa2 technology makes authentication indigenous to the image.

### 31 A Question of Logic – Statement Strength

"No alterations were discovered"
(there may be alterations we could not find)
vs
"The image is unchanged"
(a positive affirmation of authenticity)

Which statement provides more support for authenticity?

**<RESUME SPEECH SPEED>**
= = = This is the end of THE PROBLEM

= = = This is the start of THE SOLUTION

# WHAT DOES SIGNA2 MAKE POSSIBLE?

## 32 Positive Affirmation

(Stack_of_Papers, CD, “I’m authentic!”)
“Signa2” is the trademarked name of this technology.
Can provide positive affirmation of authentication for files created with Signa2 devices.

## 33 A Question of Security – Hacked

(router, locked door)
Software can be changed (hacked). Firewalls, routers, locked doors, all forms of security can be bypassed with social engineering, bribery, coercion and other tools. Could cyber-warfare include a tactic of destabilization by altering key documents?

## 34 A Question of Security – Offsite Archives

(Building_Fire)
Archives can be destroyed by fire such as the July 2006 fire in East London that destroyed an Iron Mountain warehouse. Or another fire that destroyed another Iron Mountain warehouse in Ottawa, Canada just the day before.

(Iron Mountain's fires were in July 2006. Reported in many places including Computer World on line.)

## 35 A Question of Security – Single Instance

(Stack_of_Papers, CDs)
A single instance of off site storage is not the ultimate in data security. Yet multiple instances are not possible for instances of ‘original’ documents. When Signa2 devices are used to make electronic versions then each version contains its own statement of authenticity.

## Who benefits from a solution?

## 36 A brief introduction to markets

(no voice over)

## Chain-of-custody / Law Enforcement / Legal

## 37 Chain of Custody

(show evidence_bags)
Chain-of-custody is a major market. Currently images introduced in legal proceedings have to be authenticated by a human being as actually representative of the environment in which the image was captured.

## 38 Law Enforcement (US)

(show NYPD CHP Texas)
If the image can authenticate itself then the photographer may no longer need to be present in court. Further, the ease with which digital images can be altered is rendered moot if the Signa2 authentication is present.

## 39 Law Enforcement (International)

(show RCMP Interpol German State Police)
The concept can also be applied outside the United States

## 40 Traffic Cameras

(Show picture of traffic camera)
Traffic cameras are primarily used for administrative offenses payable by fine. They are not generally used as a criminal offense with punishments such as license points or incarceration. Why? Because there are no humans the traffic cameras must be beyond reproach as they are the only evidence of the violation.

## 41 Traffic Cameras - Australia

(Show Australia_Outline)
(8/15/05 article)
In Australia all traffic camera cases are in doubt because their transit authority quote “had no evidence that an image from a camera had not been doctored.” End quote

## 42 Traffic Cameras – California / San Diego

(Show California_Outline_San_Diego)
San Diego 2001, Judge Ronald Styn ruled they were untrustworthy and unreliable. Further, the city had a participatory agreement for sharing fine revenue giving the manufacturer a clear financial motive to issue as many tickets as possible. Absent supervision or authentication the company was coining money. San Diego settled a class action law suit for more than $400,000. Was that the end?

## 43 Traffic Cameras – California / Sacramento

(Show California_Outline_Sacramento)
Nope, same thing happened in Sacramento, but the Bohl case was actually heard by the appellate court. Previous cases had been dismissed in the "interests of justice" by the district attorney to avoid a ruling on merits. For good reason, September 2004 Judge Maryanne Gilliard, writing for the unanimous decision ruled against the traffic camera system.

## 44 Intelligence Operations

(show CIA DIA FBI logos) (agencies-50)
National intelligence gathering can utilize Signa2 to reduce suspicion of altered images (or other digital files) from field sources. The technology could be embedded without notification to the intelligence resource as a control measure. Other embedded elements track the originator of the imagery automatically so there is no question as to what device was employed.

## 45 Medicine / Proactive Malpractice Defense

(liver-original-50.png)
Remember this image? Consider another MRI, misread by a doctor to the detriment of the patient. There is a tremendous incentive to alter that image to remove what the doctor should have seen.

## 46 Financial / Check Clearing for the 21st Century Act

(Check_21)
The recently enacted Check Clearing for the 21st Century Act ("Check 21") grants reproduced substitute checks the legal stature as a canceled check for purposes of authentication. In the absence of retained paper, film or fiche copies, prevention of fraud through digital tampering is a critical component in capturing the benefits of digital scanning and storage. No other authentication technology currently exists that has the ease of use and robust nature of Signa2's indigenous design because they require external software and/or trusted key sources.

## 47 Archival Information Storage

(Show Iron Mountain Logo)
Iron Mountain Corp receives $1B annually from the storage of business records. Scanning records to DVDs with the indigenous Signa2 authentication would substantially reduce their (or their competition's) storage and retrieval costs. That is just one company, there are many others. Private and governmental storage is also at risk from fire, flood, accidental disposal, termites, mold and more.

## 48 Regulatory / Sarbanes-Oxley

(show sarbox.png The Public Company Accounting and Investor Protection Act)
The Public Company Accounting and Investor Protection Act (Sarbanes-Oxley) and similar regulation expanded the volume of paper and electronic information retained by public corporations. Digital signatures and confirmations in legal and financial transactions require not only secure transmission but proof of non-tampering when viewed historically.

Further, a company may be found in violation if they can't produce transactions "on demand", rather hard to do if the company has just had a disaster.

## 49 Many Others

(show Quincy , AP logo, CNN logo, laboratory beaker)
In 1977, long before CSI, there was Quincy, ME, the model for forensic pathologists.

Other potential product embodiments include still and video cameras for forensic use, security monitoring, behavior recording, news reporting, industrial and process monitoring, testing instrumentation, manufacturing and quality control.

Signa2 automates and universalizes the process of authentication.

## 50 Size of Markets

THERE ARE 20,000 POLICE DEPARTMENTS IN THE U.S. + OTHER Federal, State, Military, Private, etc. police and investigative bodies as well as Arson and Insurance investigators, intelligence agencies and news/sports reporters + the overseas markets – we estimate an annual market of 100,000 'high-end' digital cameras per year selling in the $20,000 to $30,000 range. This does not include surveillance uses of images or the documents that never reach paper such as email; but which are subject to regulations (SarBox, HIPPA, etc.).

No one really knows how large this market could be.

= = = This is the end of MARKET. Take general questions.

= = = This is the beginning of the DETAILED SOLUTION
= = = start presentation s2-Technical

# (TECHNICAL PRESENTATION)

# 1 SIGNA2 DEFINED

## 2 Definition

From the patent
*The purpose of Signa2 devices is to acquire and record a sample of the environment in such a manner that the stored recording is verifiable as an authentic representation of the sample and has not been altered from point of acquisition in the environment. Authentication information generation capability must be indigenous to, and inseparable from, the device.*

This presentation is limited to still images

## 3 Signa2 Generic Device Model

(read the narration for the next slide)

4 The Purpose

> *The purpose of Signa2 devices is to acquire and record a sample of the environment in such a manner that the stored recording is verifiable as an authentic representation of the sample and has not been altered from point of acquisition in the environment. Authentication information generation capability must be indigenous to, and inseparable from, the device.*

## Concepts fundamental to Signa2 devices

5 Indigenous & Tightly Coupled
(show generic device model)(graphic not repeated in this document)
In this context the word means innate, inherent or native. Elements inside the thick lined indicated by 6 are considered indigenous to the Signa2 device. They cannot be separated from each other and are considered “tightly coupled”.

## 6 Signatures, definition

According to www.Dictionery.Com a signature is . A distinctive mark, characteristic, or sound indicating identity: and signature \Sig"na*ture\, n. [F. (cf. It. signatura, segnatura, Sp. & LL. signatura), from the Latin signare, signatum. 1. A sign, stamp, or mark impressed, as by a seal.

## 7 Signatures, Hancock & Forgery

Consider a well known example of an early signature.


Clearly this was the signature of the first president of the Continental Congress, perhaps the most widely recognized signature in the history of the United States. No one else made such a mark. From a veracity point of view the drawback of this signature is that it is unrelated to the document signed. It would be the same signature on the Declaration of Independence or the bar bill at Tun Tavern. Even in 1776 an unauthorized individual could manually replicate the signature. This is called *forgery*.

More than 200 years later such physical, non-adaptive, signatures can be digitized and reproduced. There are plotters that manipulate quill pens and can create signatures authentic to variable line width and differing pressure capable of creating thousands of "original" signatures.

## 8 Adaptive Digital Signature

Consider an adaptive, electronic signature. Here adaptive means that the signature changes depending on the material being signed. Electronic means that the signature is not a pattern of lines on paper, but bits in an electronic file. How the electronic signature is created is a function of the signature creation algorithm and the content of the file to be signed. **Is a representation of an environmental sample authentic, or has it been modified?** *If you can't tell therein lies the problem we're trying to solve.*

## 9 Encryption, Conventional / Key Pair

The following slides describe conventional and reverse encryption. When we're talking encryption we're talking about the non-visible portion of the image. Some of this material may appear to be counter intuitive so we're going to take it slowly. It is vital that you understand these fundamental concepts and how and why Signa2 is uniquely positioned to overcome the limitations of existing technologies.

The original purpose of encryption is to reveal the true message only to the intended recipient. This is "restricted to receiver". A key-pair is created. That is one encryption key and one decryption key. The mechanics of modern encryption algorithms differ but each key in a pair work only with each other. That is, a message encrypted with encryption key #1 (EK1) can only be decrypted by decryption key #1 (DK1).

## 10 Encryption, Conventional / Public Private

Normally the encryption (sometimes called public) key is widely available and the decryption (sometimes called private) key is tightly held. So a sender of encrypted messages to many people would need many differing encryption keys.

## 11 Encryption, Conventional / Broker to Client

(conventional_encryption)
For example: if a stockbroker wanted to send a coded message to a client:

- the message would first be created in plain text, then
- encrypted using the widely held client specific encryption key, then
- transmitted to the client, then
- decrypted by the client using the tightly held decryption key

## 12 Encryption, Conventional / Keys in Sequence

(crypt_decrypt)
While a message can be encrypted with DK1 (a decryption key) the message cannot then be successfully decrypted with EK1 (an encryption key). This is important because in both conventional and reverse encryption below one of the two keys must be tightly held. If you were able to successfully use the keys in the improper sequence the security would be compromised.

## 13 Encryption, Reverse / Authentication from Sender

Using the same basic concept in reverse we make readily available the decryption key but tightly hold the encryption key. Because the keys are paired if the file **de**crypts with **de**cryption key then it must have been encrypted with the **matching** encryption key. This is "authenticated from sender".

= = = = Optional narration
Encryption, Reverse / Authentication from Sender
So if I wanted to send a message that could only have come from me:

- the message would first be created in plain text, then
- encrypted using the tightly held encryption key (EK2), then
- transmitted to recipient, then
- decrypted by recipient using the widely held decryption key (DK2)

Since the message (or file or any digital source) is decrypted using DK2 then it could only have been encrypted using EK2. Unless the EK2 key was compromised (stolen or otherwise no longer tightly held) then the message was from the DK2 holder and is authentic. As the number of users increases, key management becomes burdensome.

It is important to remember that when we refer to encryption we are encrypting only the non-visible authentication information, not the underlying materials. That encryption is optional, but not required.

= = = = end of optional

## 14 Signa2 Device Model For Optical Recorder

= = = keep below for reference

(show patent graphic figure 2a with text below)

*The purpose of Signa2 devices is to acquire and record a sample (A) of the environment (B) in such a manner that the stored recording (E) is verifiable as an authentic representation of the sample (A) and has not been altered from point of acquisition in the environment (B). Authentication information generation capability must be indigenous (F) to, and inseparable from, the device*

= = = keep above for reference

Here is the device model for a single frame optical recorder, a digital camera. Although there are many more elements this model adheres to the six element generic device model.

## Signa2 Distinguished

### 15 Signa2 Distinguished / Not Watermarking

(international circle-slant over “Watermarking”)

Watermarking is a concept designed to clearly and continuously identify the owner, but not necessarily the sender, of an image or document. It has nothing to do with the authentication of an image. Its purpose is to preclude the generation of an unwatermarked version of the image. That is to keep the author's identification mark clear as proof of "ownership".

### 16 Signa2 Distinguished / Not Watermarking example

For example: The paper used to print currency is heavily "watermarked". If a forger could obtain the real paper the resulting currency would still be counterfeit, even though it is on genuine paper. Thus, watermarking does not guarantee the currency is authentic.

### 17 Not Steganography

(international circle-slant over “Steganography”)

In steganography bits of the pixels are altered to contain meaning. Signa2 authentication information is stored in the file without altering the substantive content of the file in any manner.

### 18 Sample Image

(S2-samp House picture)

The information in the blue band at the bottom is added internally by the device and becomes part of the image.

BECK0001 is the name of this particular Signa2 device
0028 is the sequence number of the image
142940Z is 2:29pm Greenwich Mean Time, about 8:30am in Tennessee
Global Positioning puts this at 36 degrees 26.419 minutes north and
86 degrees 22.976 minutes west.
The compass is pointing at 345 degrees
The zoom is set at 50 millimeters which is about eye-normal
Focus is set to automatic
FQ is focus quality.
It shows 10 differing points of depth ranging from 1 meter to infinity.
We're not looking at a picture of a flat picture.
The camera is at a 20 degree up angle, no flash and the file type is Tagged image format.

This is the view from my back porch looking at my uphill neighbors on a fall foggy morning in October 2005.

## 19 Levels of Authentication / TIA

Total Image Authentication is the all-or-nothing variant of Signa2 image authentication.
Authentication can yield three possible results
Unrecognized as a Signa2 image
Altered Signa2 Image
Unaltered Signa2 Image

## 20 Levels of Authentication / RCA

Row Column Authentication allows Signa2 to authenticate every image row independently, or every column independently, or both.

In this example of testing for both row and column authenticity two columns and one row failed of authentication. Because of the configuration of failure just two pixels were affected.

## 21 Levels of Authentication / ELA/DER

In the most advanced form Elemental Level Authentication is paired with Damaged Element Recovery. Every single pixel is authenticated independently. If a pixel has been altered mechanisms exist to recover its original values.

The image on the left has the same two damaged pixels as in RCA. Damaged elements are replaced by red pixels. That can be changed. For this presentation they are circled in white for easier observation. The image on the right has had the damaged elements recovered and this is indicated on the banner at the bottom.

## 22 Where is Signature Information Stored?

(show

Metadata
Past the end of image range
Visible/Human Readable in image
Visible/Non-Human Readable in image

)

Depending on the file format information may be stored in existing metadata areas or past the regular end of image market. Information may also be stored as part of the image in either human readable or non-readable format.

## 23 Where is Signature Information Stored? / File Structure

(Patent application 7A)
"Image" refers to "visible image"
Block is the source material for the signature
At a minimum there is an image and a signature.
For this example metadata space is available.

## 24 Where is Signature Information Stored? / Visible non-readable

(s2-samp-vnhr)
Where metadata space isn't available we can code items into a colored band added to the visible part of the image.

## 25 Where is Signature Information Stored? / Visible non-readable 2

(s2-same-vnhr-x)
Enlarging part of this image makes it appear blurry, but it is not. Each pixel carries distinct coding information. For these instances lossy formats would be inappropriate. Only non-loss formats would be acceptable.

The details of this encoding are beyond the scope of this presentation.

= = = = start skipping coding techniques
Translating Pixels to Numbers/Values
Bit masking techniques
Order Swap, Multi Column Barrel Roll, Diamond Shift,
= = = = end skipping coding techniques

## Adaptive Signatures, One-Time and Random Elements

### 26 Blank Image and Constant Signature

Starting with a blank image and a constant signature algorithm:
Any true image could be altered to blank and the signature from a truly blank image could be added. The resulting altered image would be improperly validated as authentic with little effort. This is a weaker situation and an undesirable outcome as the same image generates the same signature.

### 27 Blank Image with Adaptive Signature

Here a signature is generated from the contents of the image. In the case of a blank image the same signature would be generated. An image could be manipulated to blank and the signature duplicated from a properly signed blank image. This would allow the improper validation as authentic in a manner similar to the preceding. This is still an undesirable outcome.

### 28 Blank Image with Adaptive Signature and one-time elements

The addition of one time elements (never repeated elements such as date-time or image sequence number) allow for differing signatures even if the image itself is blank. Some convolution or manipulation of these one time elements is desirable to preclude their easy forgery. This is a stronger solution as the same image generates differing signatures.

### 29 The Adaptive Signature with one-time and a random element

A "random string" is a sequence of characters generated from variables including selected values from a previous image. The algorithm to create the random string is a trade secret and may differ from device to device even among the same production run of otherwise identical devices. The algorithm used may also vary from use to use of the same device. Two blank images captured a second apart with the same device can generate two widely different signatures. Two blank images captured at the exact same moment by two different devices can generate two widely different signatures. This is a stronger solution

### 30 What is a random element?

The user has control over how often a new random string is created. If the random string were created anew after each image was captured, then pattern recognition of the resulting signature from the image is not possible as by definition random elements are not patterned. Unless the signature generation protocol and the random string generation algorithm were known or reverse engineered, the ability to sign a properly constituted Signa2 image resides solely inside the Signa2 devices. By varying the random string generation protocol between devices, varying between protocols between use to use of the same device, and regenerating the random string frequently, analysis of the results to determine the process (a form of reverse engineering) is an almost fruitless exercise.

### 31 Operational Sequence Overview

# Demonstration Unit Limitations

## 32 Demo Unit

(show the Signa2 Generic Device model)

Any image capture device that incorporates Signa2 concepts will do so most effectively at the application specific integrated circuit level. In other words, it will be designed in from the beginning, not be added on to an existing system. Partly this is because add-ons are going to leave gaps in the "tightly-coupled" requirement. Attempting to replicate this for a prototype is expensive and has a limited value because no camera maker is going to do it that way. Accordingly

## 33 Demo Unit / Shoebox

(show shoebox drawing)

We've created image capture as a program executed in a portable computer. Think of the computer as the ASIC. We also have the viewer and authenticator as programs on the same machine. In the same vein we are creating a stand alone scanner with an embedded Linux operating system as an example of a Signa2 capable scanning device.

# 34 Intellectual Property

The concepts described above are protected by US patent [6,757,828 of June 29, 2004.] Various terms such as "Signa2" and ???? have been trademarked by Goldhar / Jaffe Technology Development Corporation. Other patents pending.

# 35 The End

Before Dr. Goldhar demonstrates the still image capture, are there questions?

= = = =