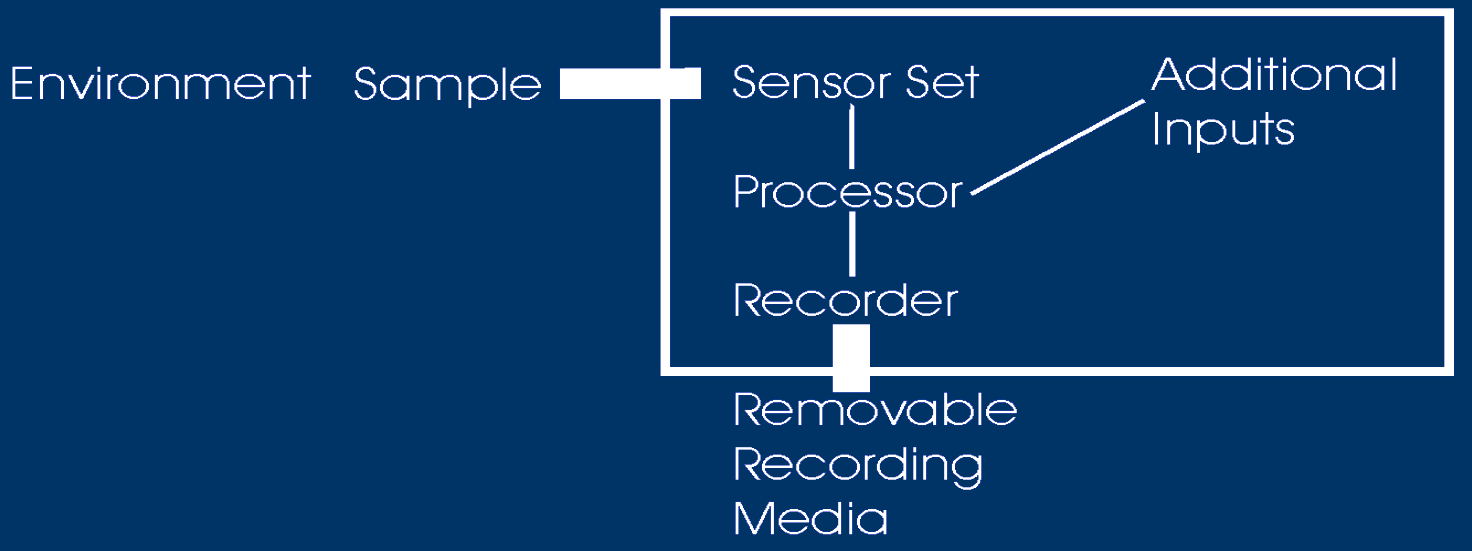
Goldhar/Jaffe
Technology Development Corporation

Signa2 Technical Presentation

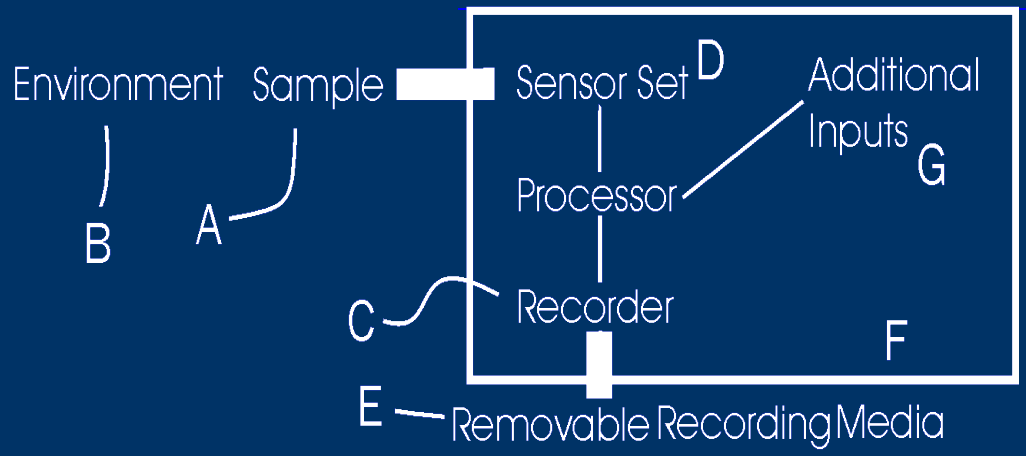
Signa2 Defined

The purpose of a Signa2 device 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.

Signa2 Generic Device Model



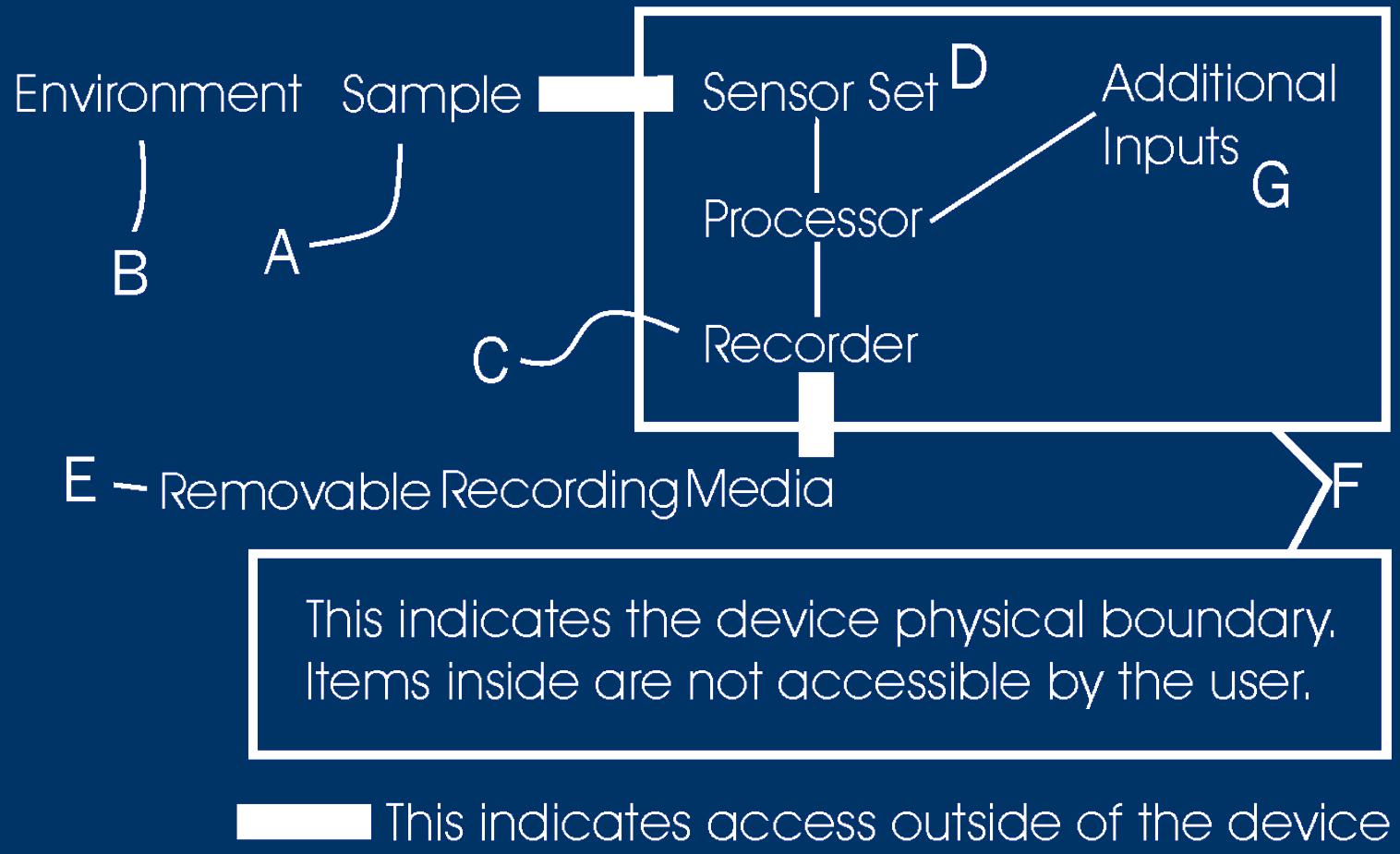
Signa2 Generic Device Model



The purpose of a Signa2 device 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.

Concepts Fundamental to Signa2 Devices

Indigenous & Tightly Coupled



Concepts Fundamental to Signa2 Devices

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.

Concepts Fundamental to Signa2 Devices

Signatures & Forgery

The signature of the first president of the Continental Congress is perhaps the most widely recognized signature in the history of the United States. A 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 230 years later physical, non-adaptive, signatures can reproduced with specialty plotters manipulating quill pens and creating thousands of "authentic" signatures with variable line width and differing pressures.

Concepts Fundamental to Signa2 Devices

Adaptive Digital Signatures

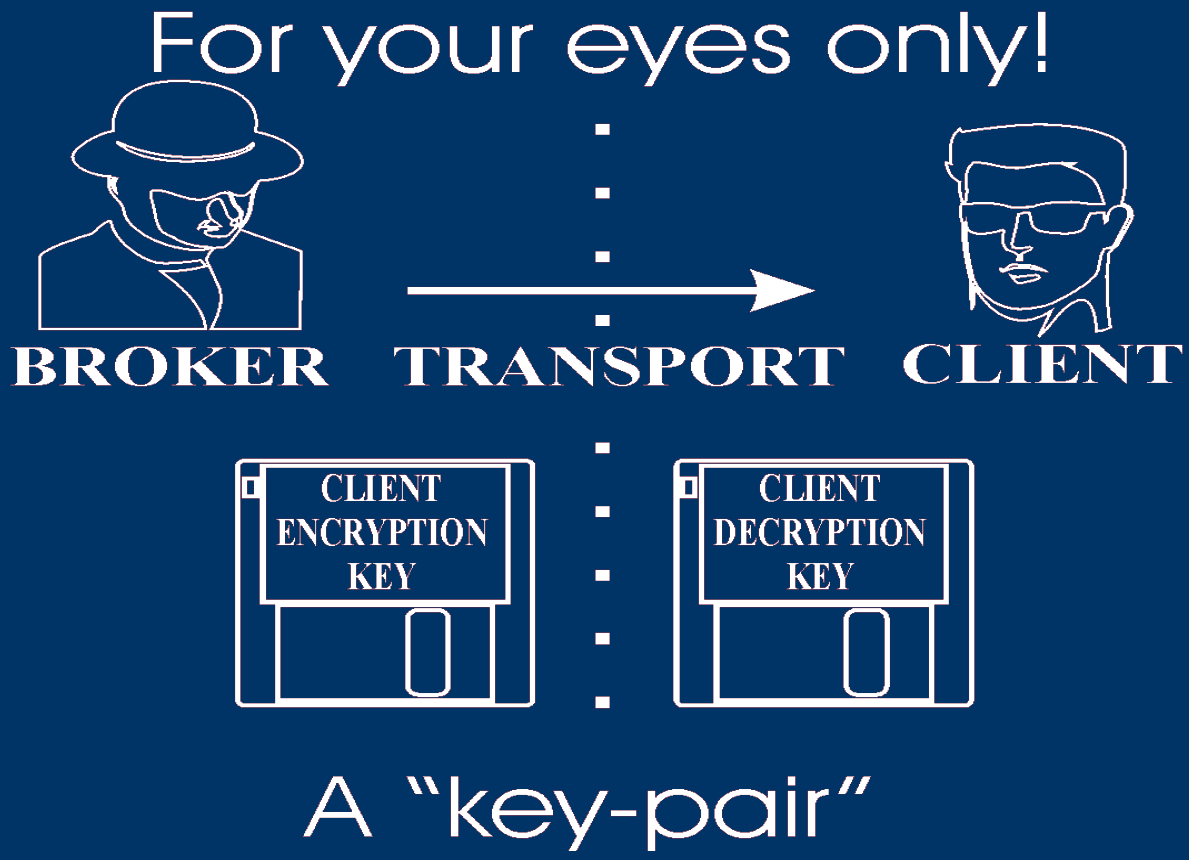
Consider an adaptive, electronic signature. Here adaptive means that the signature changes depending on the material being signed. Electronic means that the signature is not a pattern of lines on paper, but bits in an electronic file. How the electronic signature is created is a function of the signature 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.

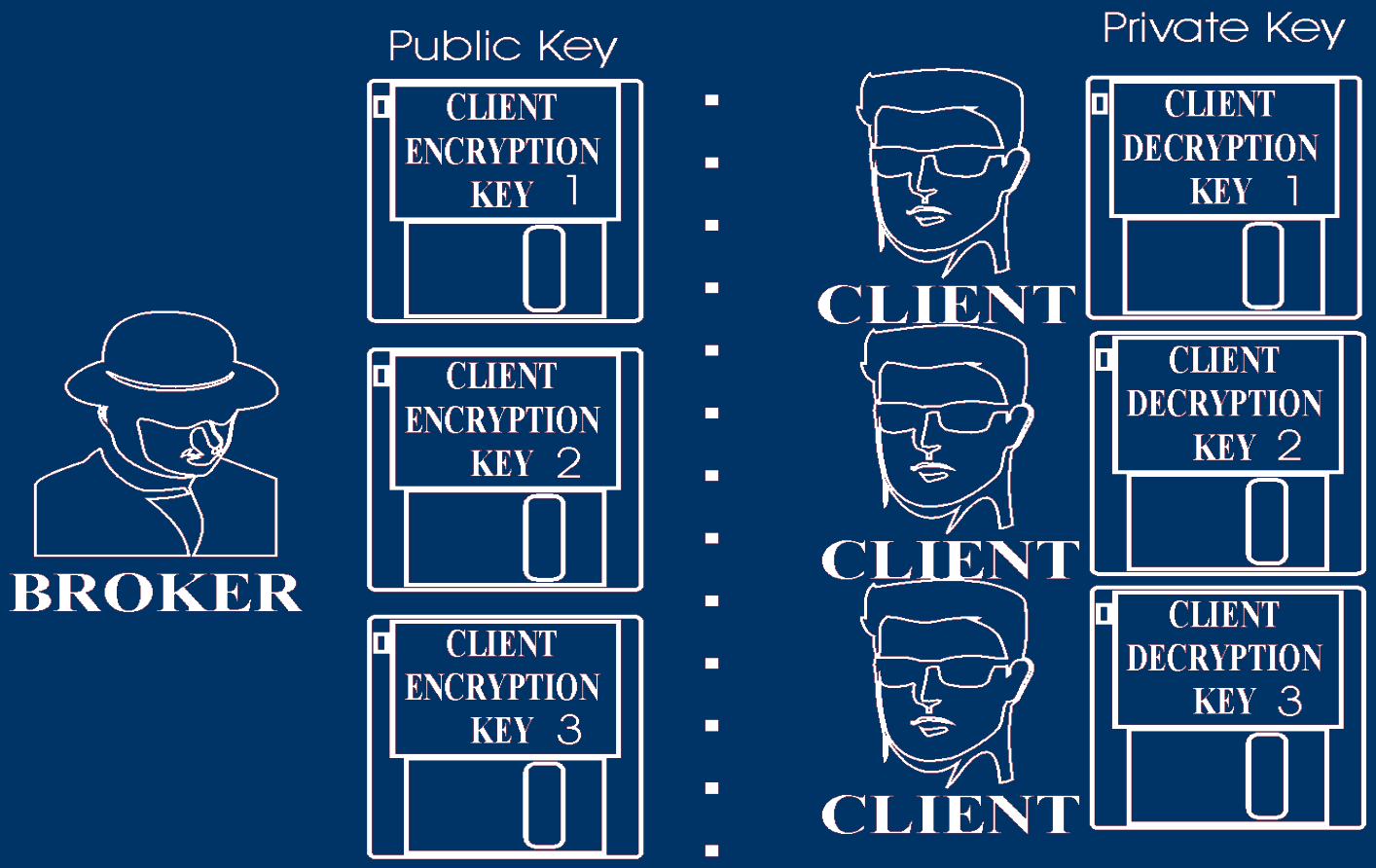
Concepts Fundamental to Signa2 Devices

Conventional Encryption



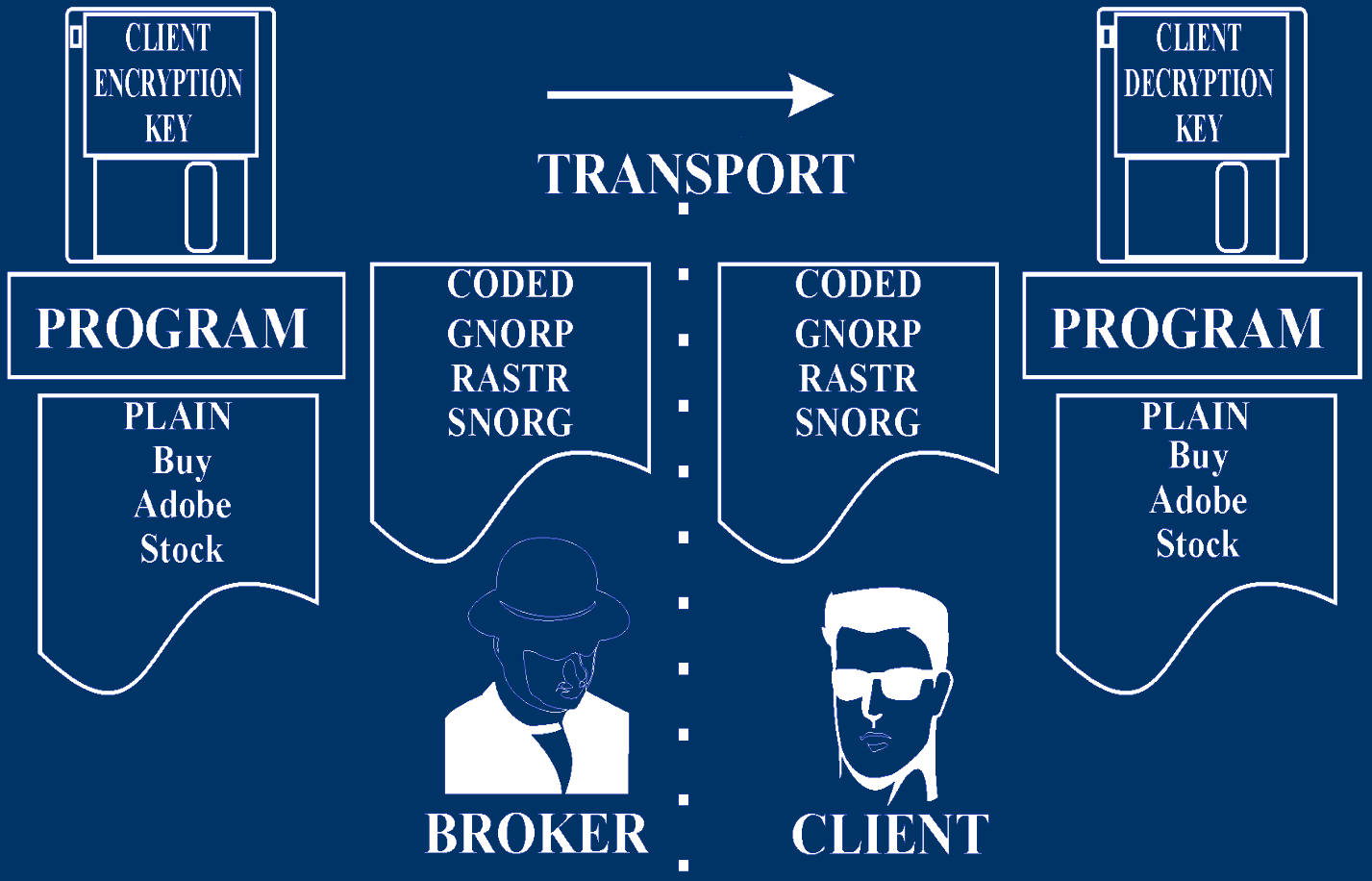
Concepts Fundamental to Signa2 Devices

Conventional Encryption



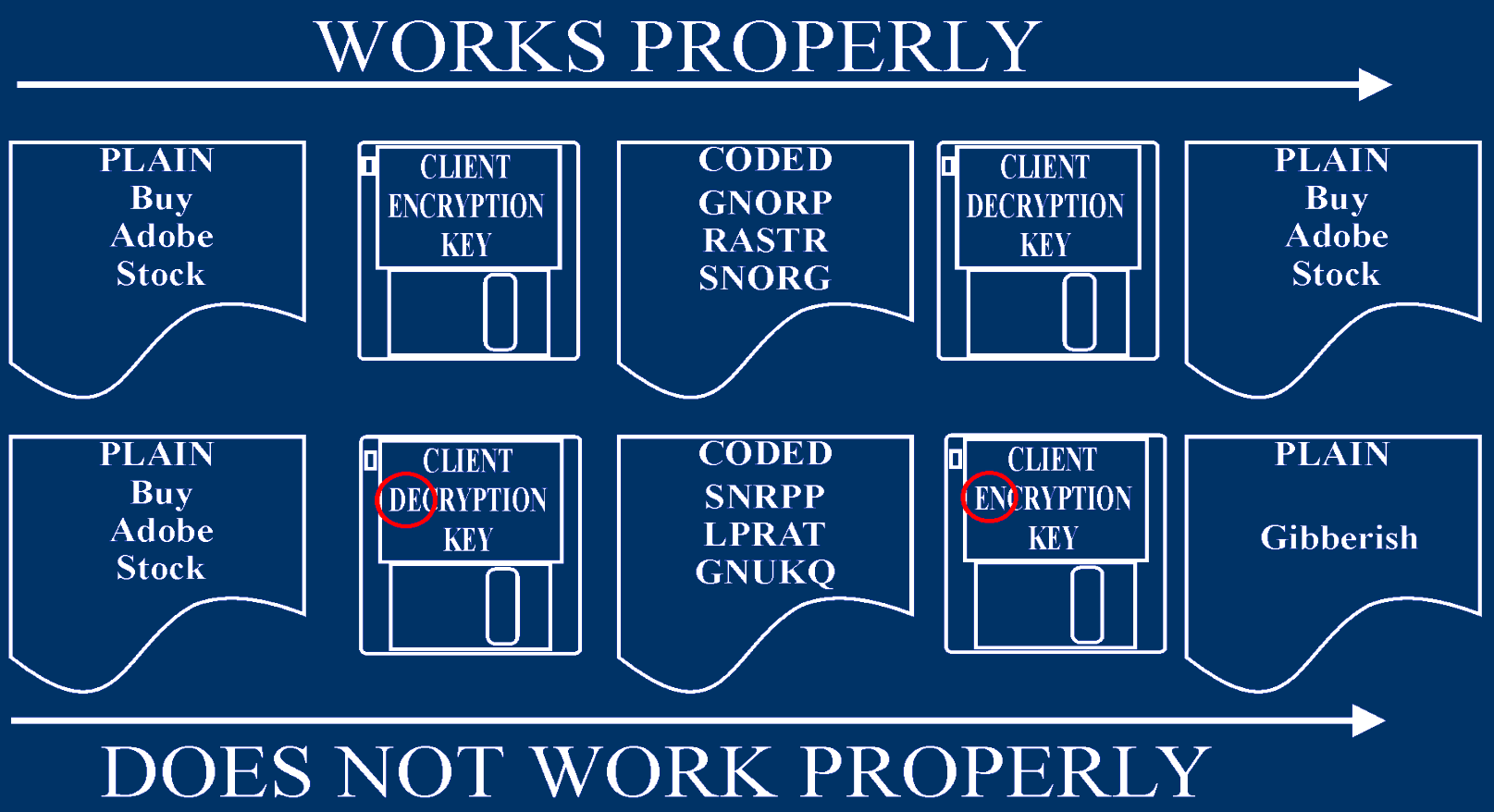
Concepts Fundamental to Signa2 Devices

Conventional Encryption



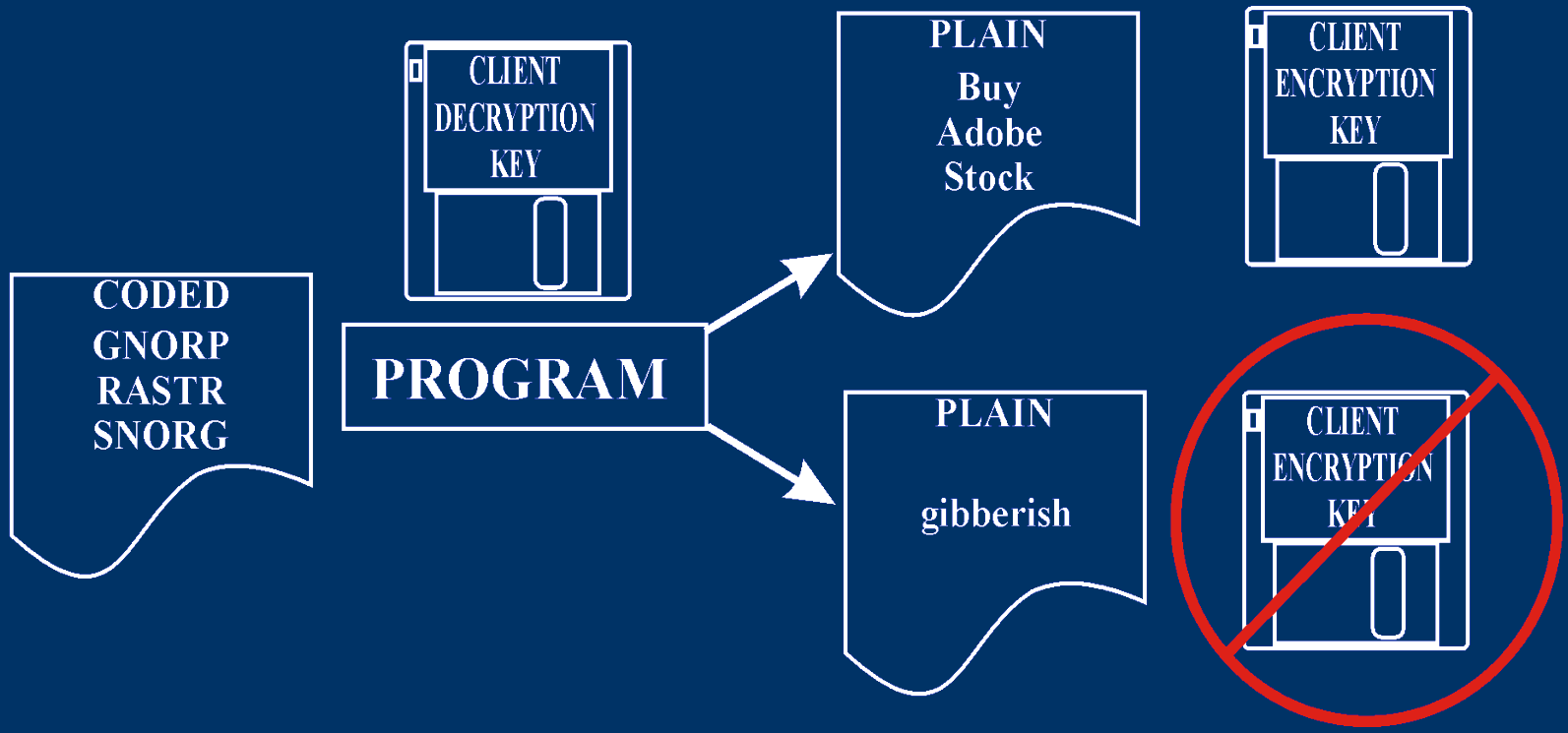
Concepts Fundamental to Signa2 Devices

Conventional Encryption

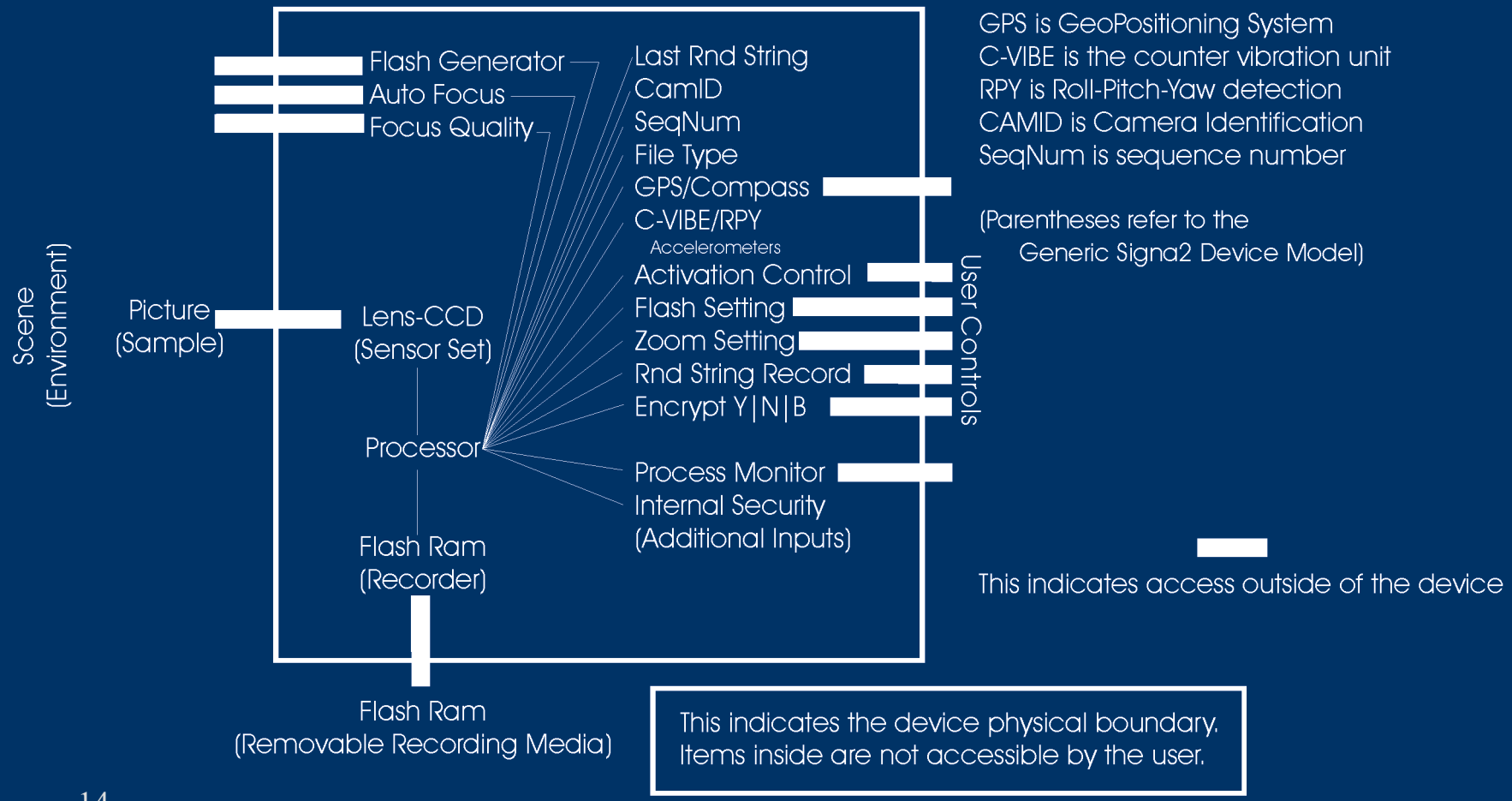


Concepts Fundamental to Signa2 Devices

Reverse Encryption



Signa2 Device Model For Single Frame Optical Recorder



Signa2 Distinguished

Not Watermarking

Watermarking is 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 to retain the author's mark as proof of "ownership".

Signa2 Distinguished

Not Watermarking

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.

Signa2 Distinguished

Not Steganography

Steganography:
where 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.

Signa2 Sample Image

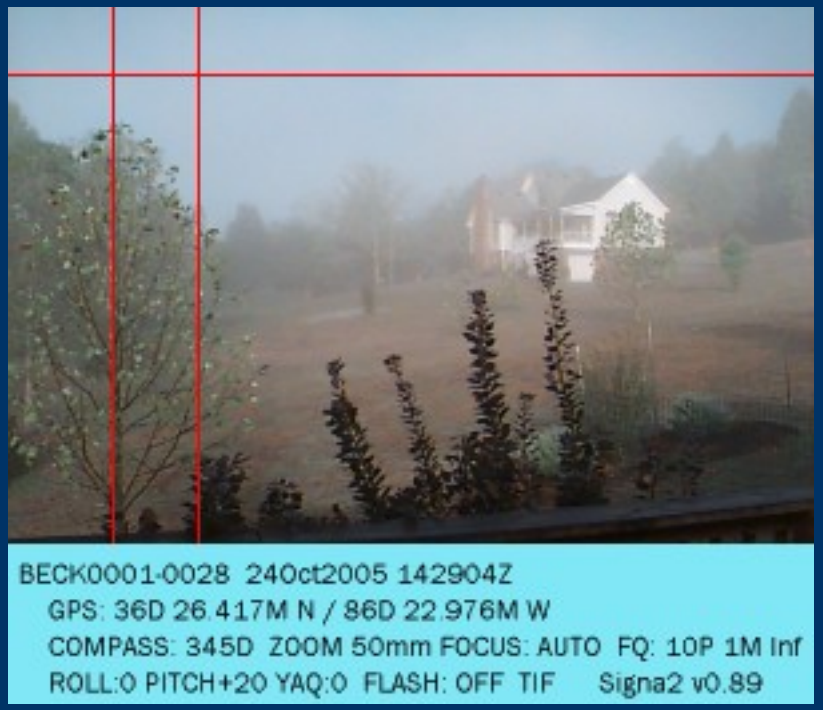
Levels of Authentication
Total Image Authentication (TIA)

UNRECOGNIZED
(can't tell if it is a Signa2 image)

ALTERED
(was a Signa2 image,
but has been changed)

UNALTERED
(is an unchanged Signa2 image)

Levels of Authentication
Row Column Authentication (RCA)



Red lines indicate a row or a column that failed of authentication.

Levels of Authentication
Elemental Level Authentication
Damaged Element Recovery (ELA-DER)

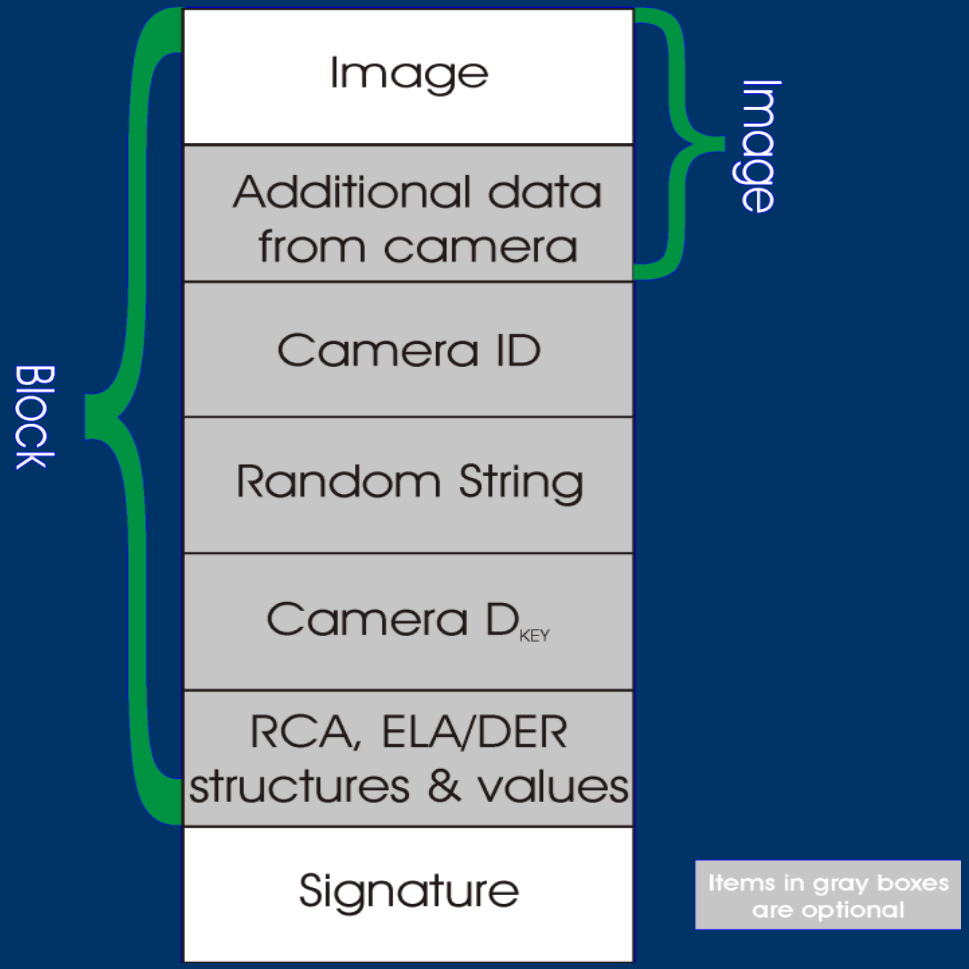
Damaged elements are circled to make them clearer in this presentation

Where is Signature Information Stored?

Depending on file format signature information may be stored

- as part of file structure metadata
- past the end of image range
- Visible/Human Readable in image
  (ex: the banner information at bottom of sample)
- Visible/Non-Human Readable in image
  (example coming up)

Where is Signature Information Stored?
File Structure



Where is Signature Information Stored?
Visible/Non-Human Readable in image

Where is Signature Information Stored?
Visible/Non-Human Readable in image

Lossy formats, such as Joint Photographic Experts Group (JPEG) would be inappropriate.

Only non-loss formats such as

Portable Network Graphics (PNG), Graphics Interchange Format (GIF), or Tagged Image File Format (TIF)

would be acceptable.

Adaptive Signatures, One-Time and Random Elements

Blank Image with Constant Signature

Signature Function is S*f*

S*f* (no parameters) = same value for any image

Adaptive Signatures, One-Time and Random Elements

Blank Image with Adaptive Signature

$S_f(\blacksquare) = 5$ (as an example)

Adaptive Signatures, One-Time and Random Elements

Blank Image with Adaptive Signature and non-repeating elements

S*f* (+DATEd+TIMEt+UNITu+IMAGEi)

= something

S*f* (+DATEd+TIMEt+UNITu+IMAGE$_{i+1}$)

= something else

Adaptive Signatures, One-Time and Random Elements

Blank Image with Adaptive Signature, non-repeating and random elements

S*f* (+DATEd+TIMEt+UNITu+IMAGEi+RND)

= something

S*f* (+DATEd+TIMEt+UNITu+IMAGE$_{i+1}$+RND)

= something else

Adaptive Signatures, One-Time and Random Elements

What is a random element?

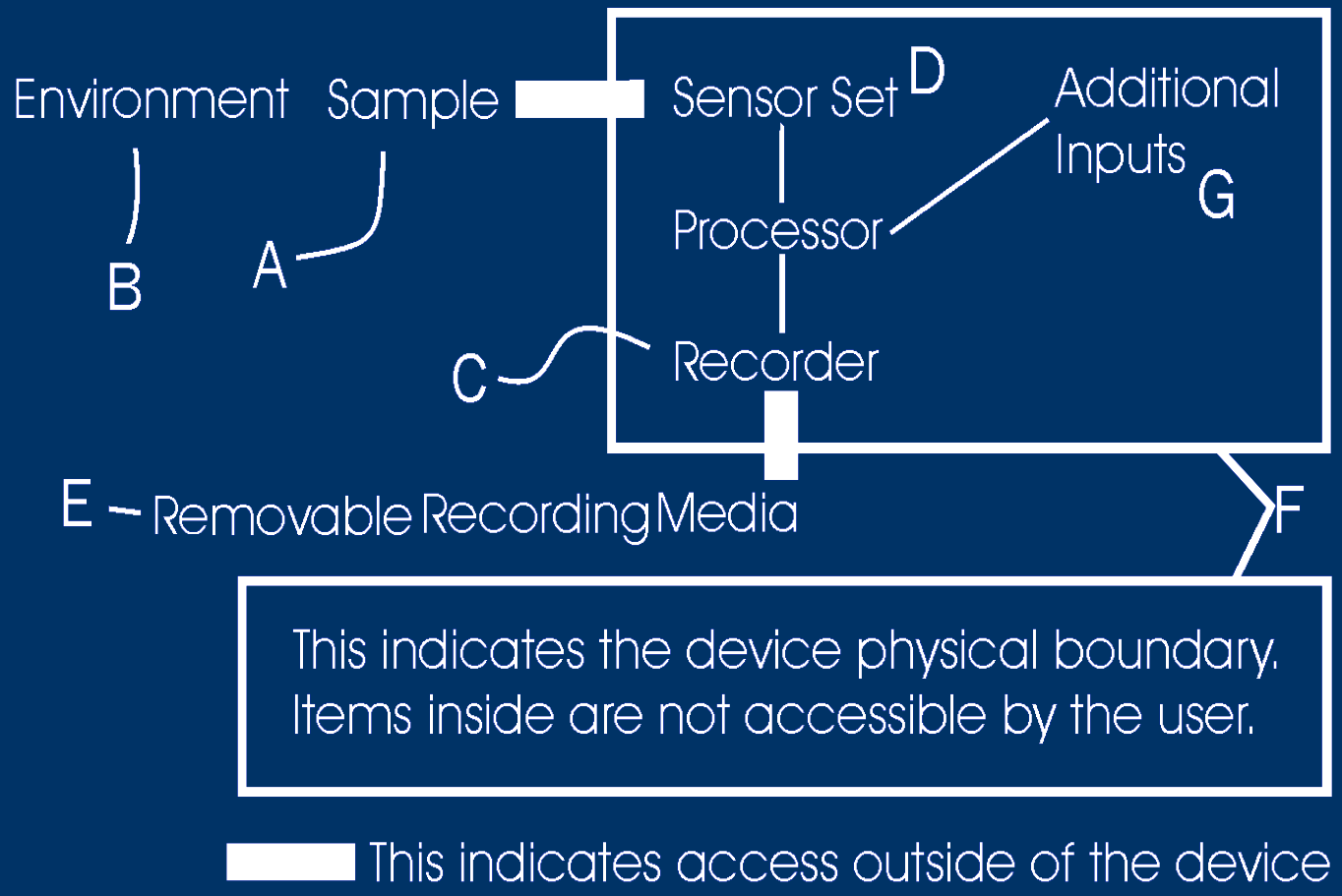
The 'random string' is the result of a function or functions applied against a value or values from the image. Which function or functions and from where in the image value or values are taken can be reset for each image.

Operational Sequence Overview

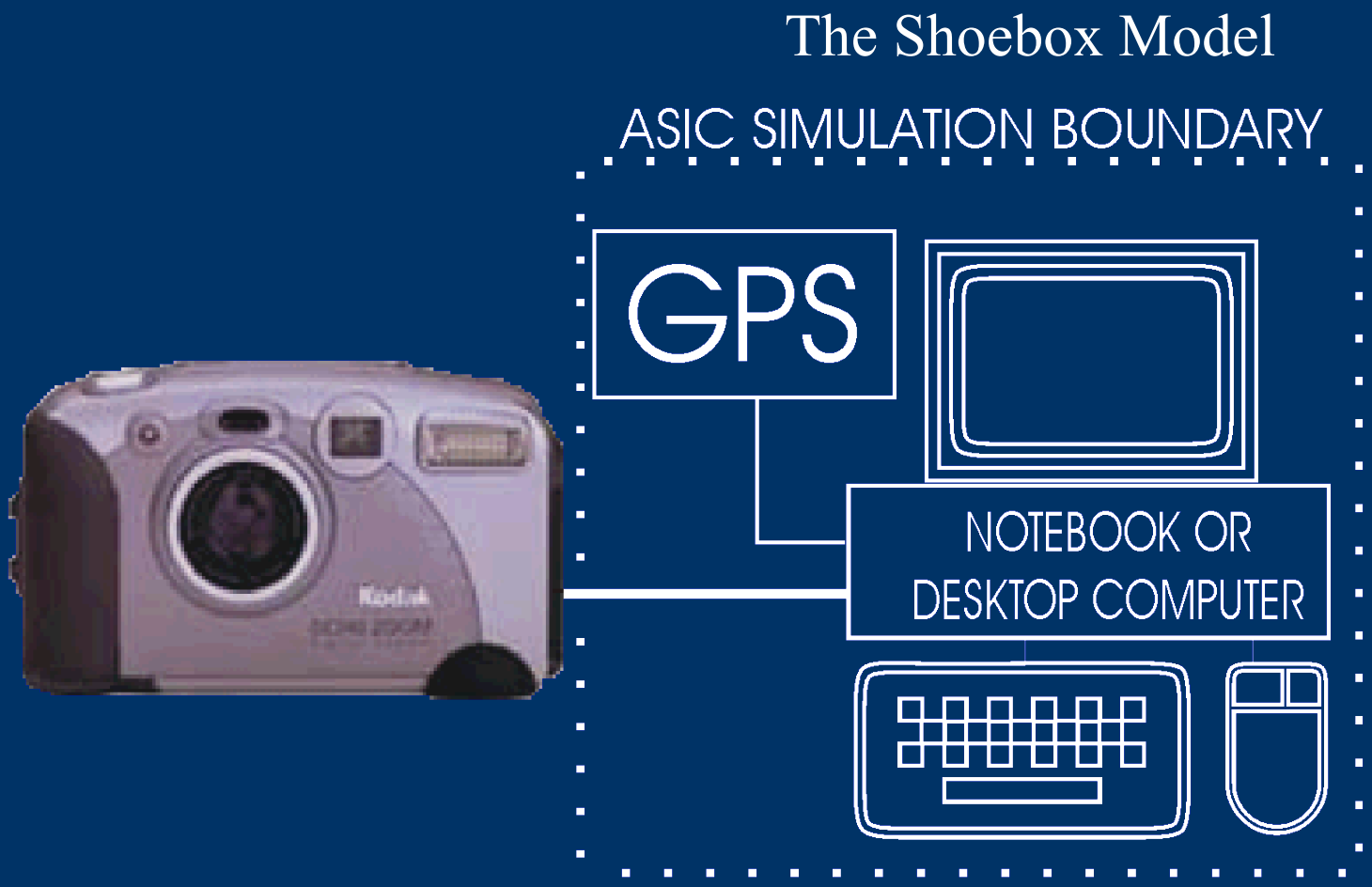
The step by step procedure of using a Signa2 digital camera and the processing steps to generate a Signa2 image are covered in the patent available on the web site at

www.gjtdc.com

Demonstration Unit Limitations



First Demonstration Unit Limitations



Intellectual Property

The concepts described above are protected by US patent 6,757,828 issued June 29, 2004.

Various terms such as *Signa2* have been trademarked by Goldhar / Jaffe Technology Development Corporation

This is the end of the technical presentation.

Questions?