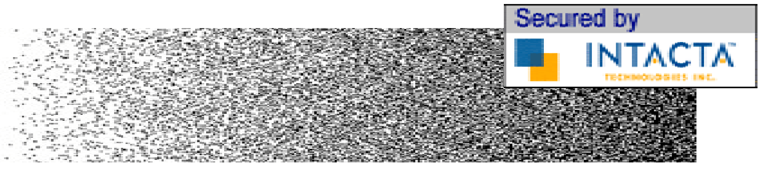
WHITE PAPER

INTACTA.CODE™

ENHANCED SECURITY MANAGEMENT (ESM)



Published By

INTACTA Technologies, Inc.
945 E. Paces Ferry Rd, NE
Suite 1445
Atlanta, GA 30326

This publication is provided as is without any warranty of any kind, express or implied, including, but not limited to the implied warranties of fitness for a particular purpose, or non-infringement.

This publication could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. These changes will be incorporated in new editions of the publication. Intacta Technologies, Inc., may make improvements and/or changes at any time to the products, technologies, and companies described in this publication.

All terms in this publication that are known to be trademarks or service marks have been appropriately capitalized. All other company/product names mentioned may be trademarks or registered trademarks of their respective holders and are used for identification purpose only.

TABLE OF CONTENTS

PREFACE

Organization Security encompasses everything from virus protection to theft control evolving from the hardcopy domain into the digital domain. It has grown from securing data to securing multi-media content on everything from an office desktop to the mobile office. The challenge for security today is to protect content from creation to archive.

This white paper introduces the underlying concepts and technologies that comprise INTACTA.CODE™ enhanced security. It is not intended to provide an in-depth view of one specific application but rather to provide the developer, Information Security Managers, and Chief Information Officer with a sense of the range of application benefits offered by the technology.

> *"INTACTA tackles the issues of security, error correction, and bandwidth efficiency. The technology, available via SDKs, takes binary data (or a combination of files),and using compression and encoding engines, it creates an envelope for the data that allows it to be distributed securely while maintaining the integrity of the format and the content. This technology was developed for the defense industry. Although their product can do more than just security, it is included here because of its potential to have an impact on the use of encryption."* IDC[1].

[1] IDC Report – Worldwide Software Encryption Market, Forecast and Analysis 2001 - 2005

CHALLENGES TO SECURITY SYSTEMS

The recent global attention on anti-terrorism has thrust Organization Enhanced Security Management (ESM) to the center stage. Security is the key focus for any organization tasked with fortifying existing policies, operating procedures, and existing infrastructure. However, any security chain is only strong as its weakest link.

Today's workplace is a complex hybrid of digital and paper information creating a broad opportunity for breach of security. *All* links in, to and from content sources must be secured. Security measures must address content creation; access control; safeguard the transmission process; and, continue its protection during its storage and subsequent retrieval.

According to a report from IDC[2], key market trends that will require enhanced measures of security are:

- Privacy. This requirement, driven by customer concerns and government regulation (see below), will encourage improved use of encryption.
- Government regulation. Government regulations (such as the Health Insurance Portability and Accountability Act [HIPAA] and Gramm-Leach-Bliley [GLB] financial services modernization law) are requiring improved security and privacy protection. Although HIPAA is focused on the healthcare industry (physicians, hospitals, and healthcare insurance providers) the financial industry is also grappling with a parallel set of privacy mandates. Stored data must be protected from unauthorized viewing, and data shared among clients, partners, and affiliates must also be protected.
- Wireless initiatives. With increasing number of devices that can access the Web, security will be paramount. Toolkit revenue (SDKs) will increase as companies develop applications for the wireless market.
- "Data at rest" protection. In 2000 there were a number of noted incidents of credit card databases being accessed by hackers. File encryption also will be used to protect data stored on PDAs that are easily lost or stolen.
- Copyright protection. The owners of intellectual property are trying to find ways to protect their property in order for it to remain valuable.

This white paper discusses how INTACTA.CODE's™ technology, provides comprehensive end-to-end security options that extend beyond the traditional digital to digital threshold. INTACTA.CODE provides a virtual "creation-to-archive" seamless security layer by encompassing digital and (hardcopy) formats that are present in every organization; and, extending its reach to any device - wired, wireless, digital or analog (fax). More importantly, INTACTA.CODE is compatible with existing legacy systems requiring additional security measures without incurring the high costs of data conversion or reengineering.

[2] IDC Report – Worldwide Software Encryption Market, Forecast and Analysis 2001 - 2005

SECURITY'S NEW ROLE

The new role of ESM arises from the need to allow a growing number of internal users to share information within the organization and outside the organization with partners, trusted vendors, financial partners, etc. This expanded information sphere means security is no longer focused solely within the organization. Today's information moves across wired and wireless Intranets and the Internet creating a fundamental change in the role of the traditional I.T. Manager from protector of the data stores, to communications controller.

Driving factors forcing realigned security measures are being created by the:

- increased physical access controls to proprietary information and facilities via biometric identifiers
- transition of the internet from an extension of the organization to "mission critical".
- increase in the mobile work force
- maintaining the integrity of paper based procedures not suited for online transition.

SECURITY CONVERGENCE – PAPER&DIGITAL

Document Security

With so much emphasis on the digital world we easily forget or simply ignore reality, i.e., 95% of the world we live in is still paper-based. The unprecedented growths of digital systems have not negated the need for equally robust paper-based security. In fact, it has opened new and greater security challenges.

The issue of hard-copy document security has grown considerably in recent years. Counterfeiting and forgeries are on the rise in the United States and abroad, making fraud a worldwide growth industry. Recent changes in the "Uniform Commercial Code" have exposed the organization to new levels of liability. As check fraud skyrockets, *the legal responsibility has been shifted from banks to account holders*, *unless the issuer has shown due diligence in protecting its checks*. According to a recent Supreme Court ruling, "the issuer of the document is held legally responsible; the omission to use the ***most effectual protection against alteration*** is evidence of neglect, which renders him responsible for the fraudulent amount." *Therefore, in the case where no security or weak security measures are in place, then the financial institution that the funds are drawn on is not responsible to cover any losses due to fraud*."

Technology Leads To Epidemic Of Counterfeiting

The same technology that is enabling organizations to reach new levels of efficiency – from computers to color copier and laser printers have made it possible for anyone to become an expert counterfeiter. FBI figures claim one million fraudulent checks enter the system **daily**, accounting for $10 billion dollars in annual losses. Fraud from checks alone is now estimated from $600 million to as high as $50 billion. In addition to check fraud, numerous other sensitive documents need protection. Documents such as; bonds, letter of credits, travel documents, identification, prescription pads, prescription labels, gift certificates, event tickets, coupons, education transcripts and confidential memo's - in short, anything that could be altered fraudulently.

The cost of document fraud to the organization far exceeds the face value of the theft. It includes even greater indirect costs. *Once fraud is discovered, there are...*

- **Direct Financial Losses** face value of financial document.
- **Cost of Investigation** employee time and disruption of normal business.
- **Settlement Costs** Legal fees involved in determining who is liable for the loss.
- **Immeasurable Costs** Loss of prestige and company image.

The Paper-Digital Divide

The notion that we are living in a totally digital world is creating false perception that if we protect our digital documents we are secure. Nothing could be further from the truth. On-line security involves more than starting and ending with a digital document. Many documents start in whole or partially from paper sources and many end in the same. Any comprehensive solution ESM for Secure E-commerce must incorporate all forms of business transactions including paper to digital, digital to paper and digital to digital - following the physical path and *form* of each

A significant discontinuity exists between paper-based and digital portions of transactions. Security exposure also exists over facsimile, still the world's most prevalent method of non-verbal communications. Use of paper is increasing and expected to grow for years to come. Many industries, such as medical, insurance, and finance, regulations require that information be kept on paper for long periods of time posing further security and privacy risks.

Any size organization must be able to transact with any other size business, anywhere in the world. Yet, little or no security solutions exist in most of these transactions, and none that enables seamless secure transactions. Not only are network specifications and operations different among businesses, quite often communication may be as disparate as between fax and computer or fax-to-fax.

ESM must be interoperable, flexible and easy to use and they must work when transactions are between known or unknown parties. Solutions must not be restrictive and allow integration of new technologies as they develop. It follows that, any secure e-commerce solution must be compatible with all platforms of the transaction. INTACTA.CODE can provide interoperability between paper and digital systems and *literal end-to-end security solutions across disparate systems.*

ENHANCING EXISTING SECURITY PLATFORMS

INTACTA.CODE is highly compatible with most other security platforms. Either used as a stand-alone security solution or as an enhancement/additional security layer or filling security gaps in existing systems. It allows developers to use it in symmetrical or asymmetrical solutions.

Additional Security Layer:

In standalone applications, INTACTA.CODE functions as encryption function and the secure carrier/packet. In complimentary applications, it can perform either function since it can include multiple layers of third party encryption. For example, in fire walls, every day organizations are exposed in the normal course of business to hostile elements both within and outside firewall boundaries. Accordingly encryption technology that enables complete encoding of all network based business communications, is necessary as a systems level service. INTACTA.CODE offers virtual private networking (VPN) capability that scales to an unlimited number of users. This function, which compresses and encrypts packets on the fly, cooperates with NSO and is transparent to other firewalls. This relieves users from encrypting individual files and e-mail messages; it also protects password exchanges. More importantly, applications do not have to be modified or re-written to support encryption standards.

Single Sign On(SSO)

INTACTA.CODE can provide a number of ways to both increase the security of SSO systems and to simplify them. These systems are often the heart of any ESM solution.

Digital Trusts

INTACTA.CODE provides solutions for both Organization and Portable Digital Trusts (mobile/wireless security) as once secured on any printable media it is unalterable. Since the current mode of Digital Trusts includes a SmartCard, the costs are only justified on higher value assets. INTACTA.CODE can provide an extremely low-cost (disposable cost) advantage opening a much larger market. In addition, current Digital Trusts do not provide authentication of the user. INTACTA.CODE can identify users and actually embed a variety of biometric data. It can also be configured for additional security to enhance current and future standards.

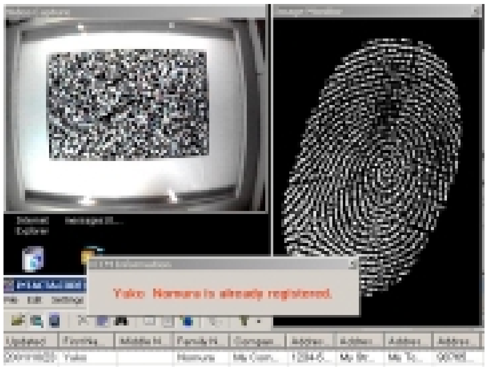
Firewalls

INTACTA.CODE provides double firewall encryption, smart hand shaking of PKI, and provides authentication and packeting. Other advantages include speed, either implemented in batch processing or real-time – INTACTA.CODE is extremely fast. Therefore, it does not reduce the throughput to any degree of significance. Flexible pricing makes it attractive for both server and mobile solutions.

Biometrics

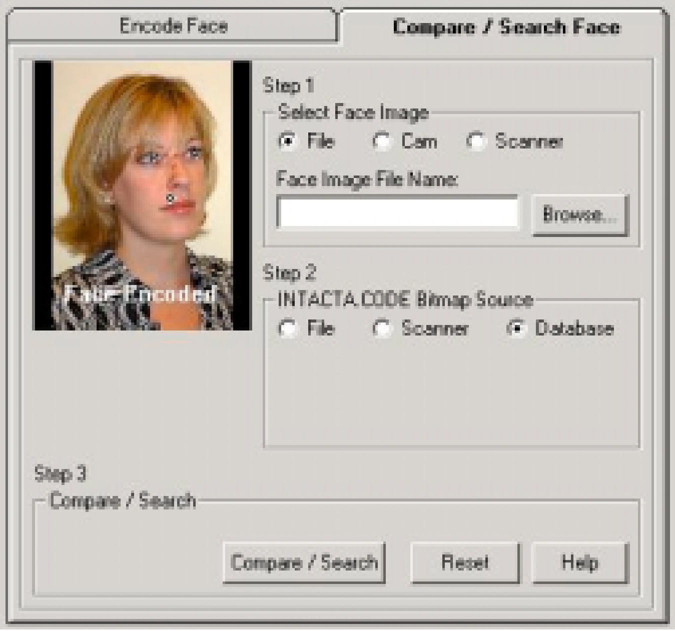
INTACTA.CODE is highly complimentary in the use of biometrics. Wrap any biometric in INTACTA.CODE and it substantially decreases the risk of interception or unauthorized use; protecting the integrity of any biometric information. The added bonus of increased compression, error-correction and the capability of transferring to paper, expands the range of biometric usability. There remains a division in standardizing interoperability of biometrics (BioApi vs Microsoft). INTACTA.CODE can not only work under both proposed standards, it could help to create interoperability between divergent standards.

The data from fingerprints, facial recognition, iris scan, etc., can all be converted into INTACTA.CODE and maintained electronically or printed on any substrate.



Yuko Nomura is already registered.

To the left is an illustration of the decoding of finger print data contained within INTACTA.CODE using a Sanyo CCD ID Card Scanner.



Select Face Image: ● File ○ Cam ○ Scanner

INTACTA.CODE Bitmap Source: ○ File ○ Scanner ● Database

At the left is a screen shot of Xpress ID 2000, an Intacta product that encodes facial recognition data for storage in a data base or for printing on an ID card. When the ID card is scanned, the data can be compared to a data base or the individual in possession of the ID card.

Multi-Factor Security

Most experts agree that there is an exponential reduction in a specific threat where multiple layers/dimensions (factors) of security are used. INTACTA.CODE enables a multi-layered, multi-dimensional approach to organization security. These factors could be a password and a randomly generated PIN, biometric data or virtually any parameter that can be uniquely associated with a specific individual.

Storage Management

The organization can configure many security barriers to prevent unauthorized users from getting into the network. However, if someone does get through, using network encryption ensures that they won't be able to read the information they find. Particularly in the pervasive environment storage security is essential.

INTACTA.CODE reduces the threats faced in storage management. The enterprise requires efficient and dependable methods of protecting and retrieving files required by applications and employees. The owners and users of corporate data, alone, can not be counted upon to adequately safeguard it. INTACTA.CODE can safely, efficiently and dependably protect the organization most valued data assets.

Hard-Copy Document Security and Authentication

Bearer and entitlement documents can be designed and produced using the most widely accepted security features, but if the people or the system responsible for their verification do not know the parameters of the genuine product the system fails and the security is wasted. (Martyn White, Product Image & Security 2/99)

Individual security approaches do provide some level of security from counterfeiting. However, they lack a total security solution that includes the four *cornerstones* of any comprehensive and effective security system: authorization, authentication, identification and content protection (integrity).

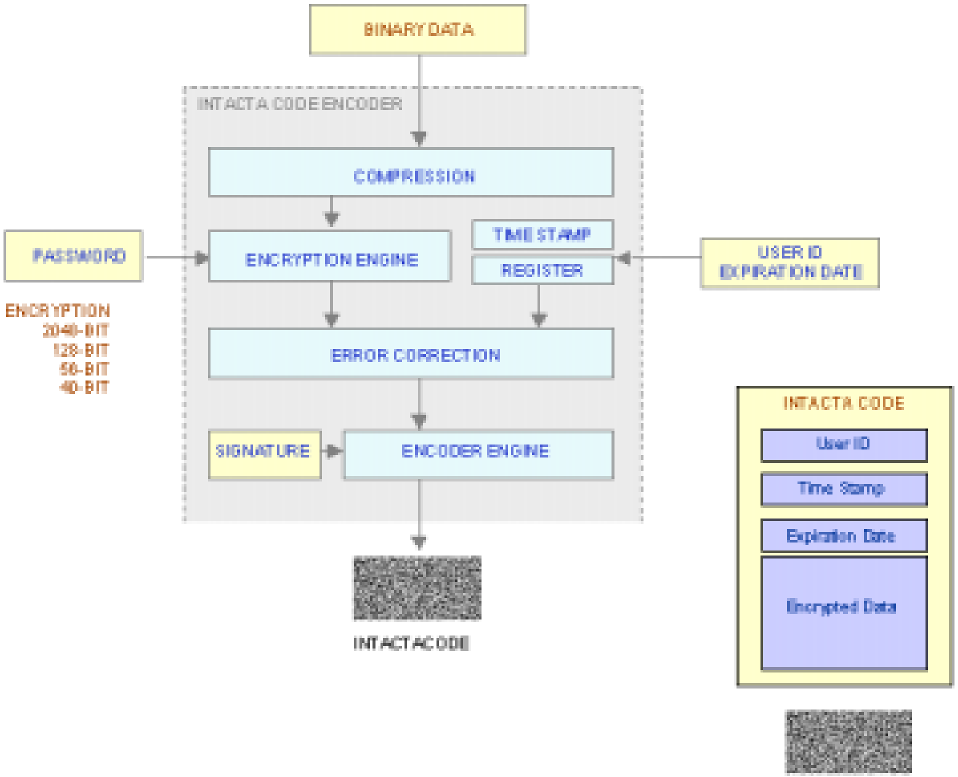
None of these alone prevents deception where the stolen originals or exact duplicate original forms are used. The use of four-cornerstone protection can appear deceivingly simple. For example, a bearer may present an authentic document - he then must prove *he* is the authentic bearer. Often other documents such as driver's license are used, which may, themselves, be counterfeit. Only by embedding individual biometrics in the document and securing separate authentication of the document, can an institution be assured that BOTH the *document and bearer* are valid. *If the form is original (i.e., not counterfeit) but the bearer is not authorized, no amount of anti-counterfeit technologies will prevent a criminal from actively proceeding.*

INTACTA.CODE provides a four-cornerstone solution. In addition to anti-counterfeit protection, INTACTA.CODE offers a complete solution combining identification and authentication with fast and simple PROCESSING. In addition, INTACTA.CODE can be printed in ghosting, ultraviolet ink, embedded in logos or other designs, microprinting, etc., to provide further security

INTACTA.CODE provides an ideal solution to protect against counterfeiting because it can be embedded within sensitive documents, labels and packaging materials.   Verification is as simple as waving a scanner over the document - a procedure so common it is use millions of times everyday.

TECHNICAL DESCRIPTION OF INTACTA.CODE

Intacta's Core Technology is founded on INTACTA.CODE. It is a patented technique of creating a graphic form for representing binary information. In this graphic representation, called INTACTA.CODE, each byte of information is represented by a small pattern of black and white or color dots. A long stream of bytes, containing one or more complete segments of information, consists of many such small adjacent patterns. A typical INTACTA.CODE appears like a random arrangement of dots, such as shown below:



INTACTA.CODE is not random. It contains 100% of the information that was written to it, together with additional, INTACTA.CODE specific, information. The INTACTA.CODE, in the above example, contains a portrait image together with additional textual information: name, address and telephone number.

Prior to creating an INTACTA.CODE the data is compressed and encrypted. The INTACTA.CODE can be created in one of two formats: Printable and Digital Format. INTACTA.CODE also has built in error correction which ensures that even if the information contained within the INTACTA.CODE container has been degraded or corrupted, the original data can be restored intact. INTACTA.CODE technology also provides this protection during file transmission and storage of the information.

A Printable Format is used where the application of INTACTA.CODE is for use on a printable media (paper, plastic cards, fax paper, etc.). In this format, the data is compressed. INTACTA.CODE can be printed using any printer having a resolution of 200 dpi or more, including fax machines. At the time of encoding, a selectable error correction factor is available. This enables the user to select higher or lower values depending on the reliability of the network or media. INTACTA.CODE is created under a process that ensures that a loss of data will not affect the ability of the algorithm to construct the original contents. The multiple levels of security that can be embedded during the encoding process makes the resulting INTACTA.CODE virtually immutable to modification and hacking ensuring the authenticity and confidentiality of the embedded content.

INTACTA.CODE differs substantially from traditional barcode. In most bar codes the data is coded in a series of bars and spaces of varying width. Ordinary barcode is "vertically redundant", meaning that the same information is repeated vertically. It is in fact a one-dimensional code.

The term matrix code applies to 2-D codes that code the data based on the position of black spots within a matrix. Each black element is the same dimension and it is the position of the element that identifies the data. A two-dimensional code stores information along the height as well as the length of the symbol. Most 2D barcodes have a fixed shape and each symbol has a maximum data capacity, i.e., although their size is scaleable, their proportions (shape) are usually fixed. For additional data to be stored requires printing additional symbols.

Although INTACTA.CODE may resemble some 2D barcode in appearance, that is where the similarity ends. Data in INTACTA.CODE is not stored in a predetermined matrix format as with conventional 2D matrix barcodes. It is randomized to enhance its error correction, storage capacity and security.

INTACTA.CODE overcomes the inherent limitations of 2D barcode including data types, data density, mixed data types, communications, security, and the need for expensive or specialized scanners. INTACTA.CODE is designed to support intelligent forms processing, fit into available size and shape of available space and to bridge the links necessary in moving any data type between hard and digital formats. INTACTA.CODE is not based on symbol architecture and therefore a continuous block of any desired shape can contain all the data.

Barcodes are designed to store a single piece or several pieces of data relevant to some form to be extracted and processed. INTACTA.CODE is the form and the process. INTACTA.CODE was developed to be independent of any specific hardware, although OEM specific versions can be customized.

INTACTA.CODE, unlike barcodes, has been designed to meet the specific demands of digital communications with advanced security and error-correction designed specifically for digital communication and content management applications. INTACTA.CODE can either replace, compliment or enhance any bar-code system, automatic document conversion (ADC) and auto-identification (AI) technologies.

The Digital Format is used for wire or wireless transmission. In this mode, INTACTA.CODE compresses, encrypts, and encodes the content. Similar to the printable format, the degree of error correction can be selected depending on the expected transmission quality (e.g., wired vs. wireless). The amount of redundant data will be added to the transmitted data for correcting errors if any, at the recipient side. Alternatively, if no errors are expected on the recipient side, pure data (compressed and encrypted and encoded) is created for transmission.

Compression

Data compression literally means making data smaller. This implies representing the same quantity of information using fewer symbols.

Data decompression means retrieving the original information from the compressed format.

Data compression is often measured by the compression ratio achieved. This is the ratio of the uncompressed size of a string to its compressed size. Other measures of data compression include the ratio of compressed bits to uncompressed bytes (1/8 of the compression ratio) or the percent reduction in size of the string.

Data compression allows increased storage of data and bandwidth throughput. In this context the compression ratio is often the most important consideration. Data compression also allows accelerated transmission of data and bandwidth throughput. In this context, when the compression and transmission are simultaneous, the speed of the compression-decompression process is important.

Compression algorithms can be divided into lossless and lossy techniques:

Lossless data compression is what we generally think of when we talk about compressing our data. It is expected that after decompression the data will look exactly as it did before compression. The problem of lossless compression has already been mentioned: not all data can be compressed.

Lossy compression on the other hand is willing to accept some change to the data after compression and decompression. This allows much greater compression of the data. Lossy compression is most often used when compressing images and multimedia.

Consider an image of 1024 x 768 pixels, each with a 24-bit value for color. If some of the pixels were to change up or down a few shades, a viewer would probably not be able to tell the difference. JPEG uses this compression method. JPEG compression allows you to select the extent of degradation you are willing to live with in order to save space.

Now consider a backup of your operating system. Backups are also often compressed to save space. In this case, you want all of your data to be restored in its original form. If one bit was changed it could be disastrous. While some algorithms are better suited to lossy techniques and others are better suited to lossless techniques, many of the listed methods could be used in either manner. It is also possible to combine the principles of each of the listed methods.

The commercial INTACTA.CODE library provides the developer with the option to either use INTACTA.CODE built-in data compression engines, or her/his preferred data and image compression engines. The built-in engine is a lossless compression engine based on Adaptive Optimizing Algorithms.

Encryption

There are two basic types of encryption systems: symmetric (also known as ``conventional'' or ``secret key'') and asymmetric (``public key.'')

Symmetric encryption requires both the sender and the recipient to have the same key. This key is used by the sender to encrypt the data, and again by the recipient to decrypt the data. The problem here is getting the sender and recipient to share the key.

Asymmetric encryptions are much more flexible from an essential management perspective. Each user has a pair of keys: a public key and a private key. Messages encrypted with one key can only be decrypted by the other key. The public key can be published widely while the private key is kept secret.

So if, for example, Mary wishes to send John some secrets, she simply finds and verifies John's public key, encrypts her message with it, and mails it off to John. When John gets the message, he uses his private key to decrypt it.
Verification of public keys is an important step.

Failure to verify that the public key really does belong to John leaves open the possibility that Mary is using a key whose associated private key is in the hands of an enemy. Asymmetric encryptions are much slower than their symmetric counterparts. In addition, key sizes generally must be much larger.

Secrecy vs. Integrity

For many users of computer-based encryption, preserving the contents of a message is as important as protecting its secrecy. Damage caused by tampering can often be worse than damage caused by disclosure. For example, it may be disquieting to discover that a hacker has read the contents of your funds-transfer authorization, but it's a disaster for him to change the transfer destination to his own account.

Encryption by itself does not protect a message from tampering. In fact, there are several techniques for changing the contents of an encrypted message without ever figuring out the encryption key. If the integrity of your messages is important, don't rely on just secrecy to protect them. Check how the vendor protects messages from undetected modification.

Key Sizes

Even if an encryption is secure against analytical attacks, it will be vulnerable to brute-force attacks if the key is too small. In a brute-force attack, the attacker simply tries every possible key until the right one is found. How long this takes depends on the size of the key and the amount of processing power available.

When trying to secure data, you need to consider:

1. How long it must remain secure and
2. How much computing power an attacker can use.

Type of Attacker	Budget	Tool	Time and Cost per 40-bit Key Recovered
Pedestrian Hacker	Tiny	Scavenged Computer Time	1 Week
	$400	FPGA	5 Hours ($0.08)
Small business	$10,000	FPGA	12 Minutes ($0.08)
Corporate Department	$300K	FPGA	24 seconds ($0.08)
		ASIC	.005 seconds ($.001)
Big Company	$10M	FPGA	.7 seconds
		ASIC	.0005 seconds ($0.001)
Intelligence Agency	$300M	ASIC	.0002 seconds ($0.001)

Time and Cost of Key Recovery

In some applications, the user may wish to employ a key-based, standard encryption algorithm to comply with his industry conventions or to gain the feeling of “higher” security.

The commercial INTACTA.CODE library allows the application developer to encrypt data before creating the INTACTA.CODE. For that purpose, the library provides the developer with the option to either use INTACTA.CODE built-in encryption algorithm, or her/his preferred third party encryption algorithm. The built-in encryption is a symmetric algorithm, DES or RC4, with the key ranging from 40 to 2048-bit.

INTACTA.CODE Secure Data Encoding/Decoding

When encoding cleartext with INTACTA.CODE, the engine compresses the cleartext first. Data compression, in addition to saving transmission time and disk space, strengthens the cryptographic security. This is due to the fact that most hackers use cryptoanalysis techniques that exploit patterns found in the cleartext to crack the ciphertext. Compression reduces these patterns in the cleartext, thereby greatly enhancing resistance to cryptoanalysis. After compression and encryption, the encoding process proceeds as follows:

INTACTA.CODE creates a partial key, which is derived from a secret key of maximum length of 256 bytes (2048 bits). This partial key (a number in the range of 1 to 2^{32}) is used as a seed to a random number generator, from which a sequence of 256 bytes that replaces the ASCII table is created. Every byte from the compressed plaintext is then replaced with another byte from the newly created ASCII table [termed new (1)], thus creating "*first step encoded data*". The number of ASCII tables that can be created in the "*first step encoded data*" is therefore equal to the number selected within the range of 1 to 2^{32}.

In the next step, the selected secret key (which can be of any length from 1 to 256 bytes), is used to create a further new (2) ASCII table that replaces the above-mentioned new (1) ASCII table. The number of ASCII tables that can be created in this step is 256! (256 factorial). The new ASCII table is used to encode the "*first step encoded data*". The encoding used is a combination of some mathematical operations, such as additions, divisions and binary XOR. The total number of possible states that can be generated using INTACTA.CODE is (2^{32} * 256! * 256^{2}) about 2^{1732} or (2.4 x 10^{521}).

Further protection is achieved by completely randomizing the cleartext; the resulting encoded ciphertext is never the same even if the same secret key and the same cleartext is used. The major advantage of this encoding approach is the fact that no keys or end-to-end compatibility are required. Moreover, "mixing" all existing ASCII character sets into one encoding table, can further enhance this method by providing more than 256! combinations. The level of security is further increased through additional operations on the bit level of the imaged byte-based information, which provides no indication for pattern (cyptoanalysis).

INTACTA.CODE Data Density

INTACTA.CODE data density depends on the resolution of the printing and scanning devices used when printing and scanning the grid. The higher the resolution, the higher the number of bytes you can encode per square centimeter.

For an INTACTA.CODE printed and scanned using 300 dpi resolution, the data density, depending on the level of error correction, is 75-140 bytes per square centimeter. When you take into account data compression, this density is translated into about 400 bytes per square centimeter for text and a much higher density for image data. At 600 dpi the data density is 371-496 bytes per square centimeter.

INTACTA.CODE Error Correction

The INTACTA.CODE technology incorporates very strong error correction. With this error correction mechanism, the content and format can still be completely interpreted even after major disturbances such as image skewing printout quality deterioration, or interference in transmission.

Quantitatively speaking, INTACTA.CODE can still be successfully interpreted after a random change to 10-50% of its pixels. INTACTA.CODE data recovery capabilities are unaffected by up to 25 degrees of skewing.

Operational Capability: INTACTA.CODE

1. Protects sensitive data from unauthorized access or use through security features, including encoding, authentication and registration.
2. COM-based components that compress and encrypt any data - such as documents, images, database records, a proprietary code that can be sent electronically over the intranet, Internet, to mobile devices. Can also be printed, faxed, and decoded, allowing secure transmission of sensitive data on printed materials.
3. Supports – EDI, X12N, Java, XML, HTML, TpaML, WML, TCP/IP
4. Designed to work with over 35 different platforms; IBM, Midrange/Mainframe, Microsoft, Sun, Unix, Linux, Palm, WindowsCE , WAP enabled Cell Phones.

Combining INTACTA.CODE with the very latest in messaging technology in a purely Object-Oriented manner (including process) provides the quickest, most scaleable and unifying method of connecting companies and organizations around the World into the supply chains of tomorrow.

CONCLUSION

A strong ESM creates a secure and confident environment for developing innovative online business opportunities. A strong ESM delivers increased revenue, maximized profitability and increased customer satisfaction through:

- Enhanced data integrity, availability and protection
- Increased employee productivity
- Extended security expertise
- Adaptive security management, measurement and metrics
- Lowered legal liability
- Improved and accelerated corporate portal return on investment

Information is the basis for competitive and strategic advantage. Therefore, managing the risk of exposure of all information content (online and *offline* and hardcopy) assumes legal importance. Organizations that adhere to a strict regimen of policy management and compliance do more than improve corporate financial performance. They also reduce the chance of legal exposures and liabilities due to negligent protection of key corporate assets.

Ensuring the availability of these key components is critical to online commercial success. When data is corrupt and systems are under attack, customers take their money elsewhere. Secure E-business is built on a strong ESM platform. Secure E-business is based on the assumption that data integrity is intact and that online systems are always available when needed.

ABOUT INTACTA TECHNOLOGIES INC.

INTACTA (OTCBB:ITAC) is a U.S. based software company headquartered in Atlanta, Georgia. The Company develops and markets software components designed to bridge organization communications and information management systems across digital and non-digital mediums.

INTACTA.CODE, the company's flagship product, is an award winning technology patented in the United States, Israel, and Europe. Platform transparent, and language transparent, INTACTA.CODE is designed to integrate with existing organization communications and information management systems requiring enhancements to security, transmission, and device handling on any number of handheld platforms, including Windows CE, WAP, and Palm OS. INTACTA licenses its INTACTA.CODE as an SDK for seamless and transparent integration within any application.

INTACTA and INTACTA.CODE are trademarks of the Company. All other company/product names mentioned may be trademarks or registered trademarks of their respective holders and are used for identification purpose only.

For more information and the latest news visit www.intacta.com.

APPENDIX A

INTACTA.CODE^{TM} FAQ

- 1) Q. What is INTACTA.CODE?

A. INTACTA.CODE is a graphic image (i.e., binary representation) of computer files generated by a patented process. This process, with a single click, compresses, encodes, error-corrects and secures any type of computer file(s). When viewed, INTACTA.CODE appears as group of black and white pixels. The resulting INTACTA.CODE, a transformation of the original digital contents, can be printed onto any document or label. When read by off-the-shelf scanners, this binary information (content) is then decoded back into 100% of its original digital content and format. INTACTA.CODE provides a new way to store, protect, authenticate, communicate and enable business processes across the paper and digital domain. INTACTA.CODE also enables secure compressed (lower bandwidth) communications across the Internet, intranets, extranets, wired or wireless, or via any other communications network including fax.

- 2) Q. How does INTACTA.CODE differ from other 2D barcode.

A. INTACTA.CODE differs substantially from traditional barcode and from the variations of 2D evolution. The terms *stacked symbology* or *multi-row code*s are more accurately applied to those symbologies made up of a series of one-dimensional bar codes. The data is coded in a series of bars and spaces of varying width. Ordinary barcode is "vertically redundant", meaning that the same information is repeated vertically. It is in fact a one-dimensional code.

The term matrix code applies to 2-D codes that code the data based on the position of black spots within a matrix. Each black element is the same dimension and it is the position of the element that codes the data. A two-dimensional code stores information along the height as well as the length of the symbol. Most 2D barcodes have a fixed shape and each symbol has a maximum data capacity, i.e., although their size is scalable, their proportions (shape) are usually fixed. For additional data to be stored requires printing additional symbols.

Although INTACTA.CODE may resemble some form of 2D barcode in appearance. That is where the similarity ends. Data in INTACTA.CODE is not stored in a predetermined matrix format as with conventional 2D matrix barcodes. It is randomized to enhance its error correction, storage capacity and security.

INTACTA.CODE’s design and functionality differs greatly from that of any 2D barcode. INTACTA.CODE overcomes the inherent limitations of 2D barcode including data types, data density, mixed data types, communications, security, and the need for expensive or specialized scanners. INTACTA.CODE is designed to support intelligent forms processing, fit into available size and shape of available space and to bridge the broken-links created in moving data between hard and digital formats. INTACTA.CODE is not based on symbol architecture and therefore a continuous block of any desired shape can contain all the data.

Barcodes are designed to store a single piece or several pieces of data relevant to some form to be extracted and processed. INTACTA.CODE is the form and the process.

Similar in concept to the PIP (picture in a picture) that you have on your TV, INTACTA.CODE incorporates DID (digital document with a document). This unique benefit permits either the original hard copy document to be embedded in a digital form or to embed an entirely separate companion form (e.g. invoice and related PO, packing list and BOL, etc.. INTACTA.CODE enables the user to create any type of Intelligent Form for moving data or executing other functions within or between enterprise forms.

Most barcodes were developed by hardware manufactures to promote the sale of their systems. INTACTA.CODE was developed to be independent of any specific hardware, although OEM specific versions can be customized.

INTACTA.CODE, unlike any barcodes, has been specifically developed for digital communications. Similarly, Intacta has developed advanced security and error correction designed specifically for digital communication and content management applications. INTACTA.CODE can be used in replacement or as a compliment and enhancement to any bar-code system, automatic document conversion (ADC) and auto identification technologies by increasing the level of performance data integration.

- 3) Q. You state ANY kind of data or content can be embedded. Do you really mean any? Can I, for example, store a voice message, or photo?

A. YES. INTACTA.CODE is fully *multimedia* compatible. You can store any type of information that you normally store on you computer, including voice, music, executable codes (macros, software agents), photos, video clips, biometrics, signals, etc. Anything that can be stored as binary file can be store embedded in INTACTA.CODE. In addition, INTACTA.CODE enhanced versions allow a mixture of data types. For example in the same INTACTA.CODE block you can store a sound file, text file, executable file, and an image.

- 4) Q. If I store a document in a specific file format such as Oracle, Excel, Word, etc., will I loose my original format when I retrieve the data back?

A. On the contrary, INTACTA.CODE is designed to deliver you content and format unchanged. You will maintain 100% of your original document format. This is an extremely powerful benefit when used to transfer information from paper to digital systems or from digital-to-paper-digital.

- 5) Q. How much data can I actually store?

A. The actual amount of data or content that can be stored in a given space is dependent upon 3 variables. 1) The level of compression (varies with the type of content, e.g. text vs. image); 2) the printing resolution, and, 3) the optical resolution of your scanner. Typically, 110 kilobytes of digital data (approximately 100 pages) can be embedded as a single page (8.5 x 11) at 300 dpi print and scanning resolution. The above figures refer to the *after-compression* file size. Just like you HD, FD, or CD, the size of the file before compression is often many times greater.

- 6) Q. What does this translate to in bytes per square inch (BPI)?.

A. The mathematics involved is non-linear. For example, the effect of increasing the print/scanner resolutions equals approximately (assuming equal printer/scanner resolutions):

1000 BPI @ 300 DPI
1400 BPI @ 400 DPI
3800 BPI at 600 DPI

- 7) Q. Isn't this the same as document conversion using some form of OCR?

A. NO. OCR is the process of document conversion in which *static* content is imaged and then attempted to be matched against stored templates in the effort to convert it into the proper digital representation. This is an extremely complex task. And although OCR can work reasonably well under ideal circumstances, the reality is that files usually contain various errors and formats changes or losses. In many applications the loss or addition of a period, for example in numerical use, can be disastrous. Where a high degree of accuracy is reached by OCR, the solution requires the implementation of very expensive and complex systems and they still cannot achieve 100% of content and format on a 100% consistent basis.

INTACTA.CODE enables ADC (Automatic Document Capture) by transforming the static document into a dynamic document through a process we call OFRtm – Optical File Recognitiontm. With INTACTA.CODE, the actual digital document is embedded on the hard copy is scanned. The result is ALWAYS 100%. The patented algorithms used to encode/decode INTACTA.CODE virtually prevent - 100% of the time - a file from being opened if even a SINGLE error or format change has occurred. This guarantees that any decoded INTACTA.CODE file is virtually 100% accurate 100% of the time!

- 8) Q. I have heard about other new codes, such as GoCode, CueCat, etc., What is the difference between INTACTA.CODE and these new web-enabling codes?

A. These technologies were designed primarily as single or 2D barcodes that simply contain a URL. The have the same inherent limitations as other barcodes discussed above. In a nutshell, INTACTA.CODE can provide the same functionality as any of these codes. *None of these codes can provide functionality equal or even approaching Intacta.Code.*

Use our Free Reader to Open the Comparison Chart.

- 9) Q. How does INTACTA.CODE compare with RFID?

A. RFID is a passive electronic component that can omit an RF signal without direct line of sight. It is much costlier per unit than barcodes, but can be reused. INTACTA.CODE can embed the frequency of an RFID to maintain compatibility between disparate technologies and works as a strong compliment to this technology.

Creating and Decoding INTACTA.CODE

- 1) Q. How do I create and retrieve an INTACTA.CODE file?

A. INTACTA.CODE is comprised of a Compression Engine and an Encoding Engine. The Compression Engine takes the selected computer file(s), and compresses them using binary compression technology. INTACTA.CODE reduces the overall file size, with 100% assurance of complete file restoration by reversing the compression process.

The Encoding Engine encodes the resulting file(s) into a binary grid pattern of very dense dots, called an INTACTA.CODE while simultaneously embedding a proprietary error correction algorithm to aid in the accurate recovery of the data.

The Decoding Engine contains the software required to read the INTACTA.CODE and restore the data back to 100% of its original computer file format.. The INTACTA.CODE creates a secure, reliable and efficient duplicate of the original digital file.

- 2) Q. What type of printer and resolution is required to print INTACTA.CODE?

A. Any type of printer can be used (thermal, ink-jet, laser, dot matrix, etc.) as long as the print resolution is equal or exceeds to optical resolution of the scanner.

- 3) Q. We have many different forms that we do not want to redesign. How can INTACTA.CODE fit into our existing legacy forms?

A. There is no limitation on the boundaries or shape of INTACTA.CODE. Therefore, if there is any existing open space available on your form then INTACTA.CODE can be easily printed with those confines. If no space exists, then a second attached page can be used.

- 4) Q. What medi*a* can INTACTA.CODE be printed on?

A. INTACTA.CODE can be printed on any printable media including conventional paper forms, newspapers, magazines, Tyvek, Teslin, plastics, etc.

- 5) Q. Is it true that INTACTA.CODE can be read by almost any scanner, even the cheap ones I received with my PC?

A. YES, INTACTA.CODE was specifically designed to be used with any linear or CCD contact scanner (refer also to B.8 below), including the lowest resolution scanning device, i.e., fax machines with resolutions that are only in the 100-200 dpi range. In general, any 300-dpi optical resolution scanner, can be used effectively.

One of the major drawbacks with 2-D barcodes, is the cost of scanning equipment. Printing a 2D barcode is the same cost as standard barcodes. The largest differential is in the cost of scanning. This problem was overcome by building into INTACTA.CODE an extremely robust error-correction. Since error-correction is embedded within the data, INTACTA.CODE is as reliant upon a specific's scanner's error-correction, enabling virtually all types of scanners to be used.

- 6) Q. If I use a higher resolution scanner, can I increase the amount of data I store in the same space?

A. Yes (refer to question A.6), if you *print* and *read* at the higher density. INTACTA.CODE's density is subject only to the limitations of printing and optical scanning technologies used. INTACTA.CODE can read millions of DPI provided the printing and optical resolution are equivalent.

- 7) Q. Your density and use of almost any scanner is impressive. But how practical is it for use under severe conditions of the real world. Our documents get dirty, crumpled and torn. What good is all this storage if I cannot retrieve it.

A. INTACTA.CODE has proven itself under some of the most difficult conditions. The world's largest newspaper publisher chose INTACTA.CODE after more than a year of exhaustive testing. INTACTA.CODE was selected to embed new interactive content in their daily publications. Normal barcode labels and packaging is usually very durable. Newsprint, as we all know, is very fragile. INTACTA.CODE is designed to overcome these challenges with rigorous error correction technology built-in. Crumpled, stained and even torn INTACTA.CODE can, in most cases, be read. INTACTA.CODE is so robust that it can recover 100% of the contents successfully after random destruction of as much as10-50% of the printed INTACTA.CODE and withstand up to 35 degrees skewing (of the document).

- 8) Q. It is not practical for us to use contact scanners in our application. Can contactless scanners read INTACTA.CODE?

A. YES. Intacta Technologies is working with a number of hardware manufactures of contactless scanners and CCD cameras to offer customers with a wide range of scanning/imaging options. A list of these manufactures and models will be available on our Website once full testing has been completed.

INTACTA.CODE Compatibility within The Enterprise.

- 1) Q. I am impressed with INTACTA.CODE's capabilities. However, I have specific application in mind that will most likely require a high degree of customization. How can INTACTA.CODE help me.

A. INTACTA.CODE is designed as a middleware product. We have developed a range of DLL libraries that our engineers can use to tailor INTACTA.CODE for your company's specific requirements and for your engineers to easily integrate INTACTA.CODE into any of your products or applications.

- 2) Q. Yes, but what if I need more customization than offered within your DLLs?

A. Intacta Technologies, offers custom project development services. We can design and optimize custom DLLs to meet your company's specific objectives.

- 3) Q. Our company is developing a number of wireless and mobile applications to allow supply chain management anywhere, anytime, anyplace. Is INTACTA.CODE compatible and how can we provide enhanced benefits to our customers.

A. Pervasive or Ubiquitous computing over wired and wireless media to thin client is an exploding area of our New Economics. However, several key challenges are presented. These are: end-to-end security as many supply chain documents may be sensitive; bandwidth, error-correction and storage capacity. INTACTA.CODE provides extremely strong end-to-end security. It is the first technology approved as a plug-in transcoder to IBM's Websphere for store and forward security between IBM servers thin clients (e.g Palm). Our compression and error correction helps conserve bandwidth during transmission and storage space on the thin client. Our error correction helps ensures that the information is received with 100% accuracy. NTT, the world's largest telecom company has chosen INTACTA.CODE for its wireless communications in areas where the sender is moving such as in bullet trains, ships, etc.

- 4) Q. We would like incorporate INTACTA.CODE within a PDA to work with scanner attachments. Will the PDA have enough computing power? What is the average space required to run INTACTA.CODE?

A. INTACTA.CODE requires minimum processing power which is below any of today's or even the first generation PDA or Information Appliances. Depending on the specific functions required, INTACTA.CODE will run in memory as little as 25-50K.

- 5) Q. *T*here are many existing platfor*m*s and standards existing and new ones emerging. Is INTACTA.CODE compatible with the existing ones and how will you maintain compatibility with emerging ones?

A. INTACTA.CODE has been modularly designed to enable implementation across any platform and compliance with existing or future protocols or standards. In most cases, INTACTA.CODE operates completely transparent to the end user. Our design enables full scalability as well as backward integration/compatibility with legacy systems and forward compatibility to accept the latest technology enhancements. Our engineering division is continuously working to ensure that INTACTA.CODE will meet your needs now and in the future.

**The INTACTA.CODE below contains this entire document with compressed and encrypted. It was created with a simple “plug-in” developed for Microsoft Word 2000®.