

288 Bishopsgate  
London EC2M 4QP  
United Kingdom

Tel: +44 (0) 20.7959.3010

Fax: +44 (0) 20.7959.3090

**evident**  
technologies™

## Digital Evidence

63 Pitts Bay Road  
Hamilton HM08  
Bermuda

Tel: +1.441.295.1639

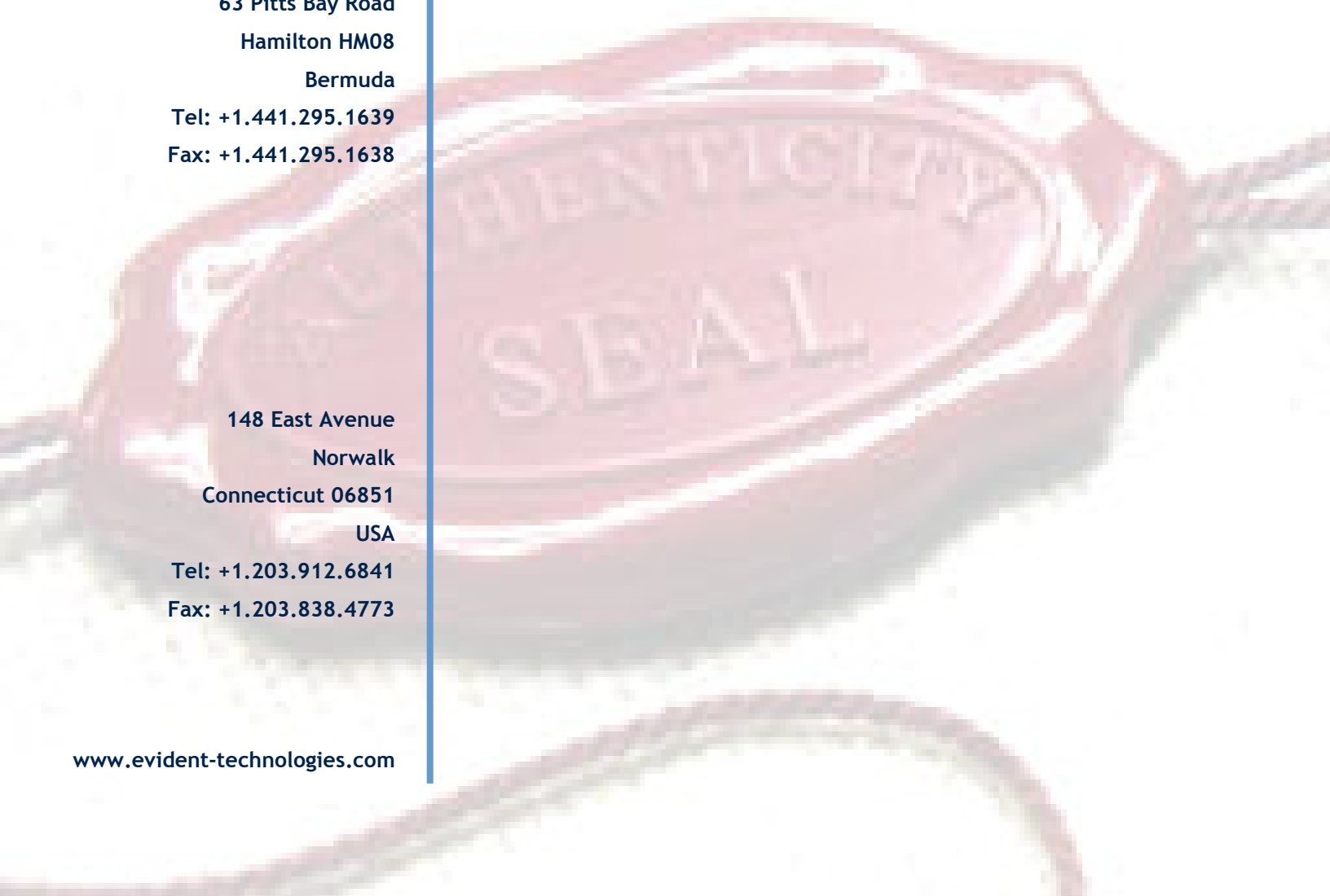
Fax: +1.441.295.1638

148 East Avenue  
Norwalk  
Connecticut 06851  
USA

Tel: +1.203.912.6841

Fax: +1.203.838.4773

[www.evident-technologies.com](http://www.evident-technologies.com)





# Contents

The principles, legalities and technical features behind the only digital evidential product currently in the marketplace that provides durable and conclusive evidence of any electronic document or transaction

## Evidence Seals™

### Introduction

|                                  |   |
|----------------------------------|---|
| What is an Evidence Seal™?       | 3 |
| Key Evidential Features          | 4 |
| Business Benefits                | 5 |
| Why Digital Evidence? - Why Now? | 6 |
| Why not Digital Signatures?      | 7 |
| Legal Features & Ramifications   | 8 |

### Technical Overview 9

|  |    |
|--|----|
| Sealing Operation - <i>Detail</i>        | 10 |
| Sealing Operation - <i>Graphic</i>       | 11 |
| The Evidence Seal™                       | 12 |
| A Sealed Document with Validation        | 13 |
| Evidence Manager™                        | 14 |
| Applications - <i>Evidence Toolkit™</i>  | 15 |
| Applications - <i>Packaged Solutions</i> | 16 |

### Summary 17

**Non-repudiation** is the ability to ensure that a party to a contract or a communication cannot deny the validity of the contract or of a communication that they originated. In today's global Internet economy, where face-to-face agreements are often not possible, businesses and regulators are increasingly aware of the vital need for electronic non-repudiation

## What is an Evidence Seal™?

A simple piece of XML based data which is cryptographically appended to any digital data, over any digital medium.



The Evidence Seal™ proves, indisputably, over time;

- Who were the parties involved
- What the original information or data was
- When the event happened

**Evidence Manager™** is a stand alone network appliance that provides **Evidence Seals™** to data, via a corporate solution or managed service, assuring the evidential value of any electronic transaction or document.

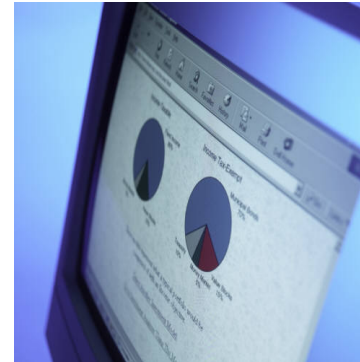
## Key Evidential Features

The Directors and Corporate Advisors' Guide to Digital Investigations and Evidence, published by the IAAC, warns that businesses are ill-prepared to provide digital evidence to prove regulatory compliance and to defend themselves against possible corporate prosecutions

- **Validation** - The authenticity of the data is independently verifiable
- **Integrity** - Changes to the original data are immediately detectable. It can be proven that the data is in its original form and can be treated as a true original - *The Gold Copy*
- **Durability** - A unique process of re-sealing using the latest strength cryptography ensures that evidence endures for a long period of time
- **Transparency** - Evidence is presented clearly and unambiguously in a user-friendly, human readable form
- **Portability** - Whenever the data is sent, copied or moved, it's authenticity can still be independently verified

## Business Benefits

- A unique and unrivalled evidential technical offering, positioning any organisation above repudiation and ensuring that electronic trading and negotiation never suffers from expensive and time consuming evidential disputes
- The ability to engage with all sectors of the global market while being assured of the evidential strength, quality and durability of your data and communications
- Changes to protected data are immediately detectable. It is possible to prove the data is unique and can be treated as a true original in the same way as a paper document
- Supports evidential regulatory and legislative requirements and provides your clients with absolute confidence and trust in the authenticity of your electronic data
- Seamless integration with existing business processes, applications and user authentication schemes delivering non-intrusive and automatic sealing
- Full conformity to UK, US and European privacy and evidential legislation
- The authenticity of electronic data is independently verifiable therefore providing non-repudiation properties. Even if the originator denies having created the data, the truth can be independently and irrefutably demonstrated



Organisations need a digital evidence plan

“It’s frankly astonishing that businesses are not doing this. It’s no different to having a security policy. Businesses look at tackling spectacular events, such as floods, hacking or the effects of terrorism, but fail to focus on the importance of digital evidence for events that happen all the time”

Peter Sommer  
Senior Research Fellow  
London School of Economics

## Why Digital Evidence?

- Organisations today rely heavily on electronic communications, documents, scanned data, and the electronic storage of business records
- Even the best communication, scanning and record-keeping processes cannot ensure that electronic data maintained inside or delivered outside of an organisation's systems, maintain proof of their authenticity
- The inability to provide adequate evidence of the provenance and authenticity of electronic data results in the failure to withstand challenges to the data's integrity
- These cases, often settled out of court, can result in significant costs, and, where they become known, in a loss of confidence and the undermining of business reputation

## Why Now?

- Failure to provide adequate evidence of the provenance and authenticity of electronic data could result in a failure to prove the data's integrity if challenged by regulators, in a business dispute or in court
- Such challenges are now widespread and can often occur many years after the event in question
- Knowledge of the exposures of electronic data is now commonplace and the integrity of any electronic data will be contested whenever disputes or disagreements occur
- In an increasingly regulated scrutinized and litigious world, now more than ever before, companies need the ability to irrefutably prove the provenance and authenticity of their electronic records

## Why not Digital Signatures for Evidence?

- Over time, cryptographic keys will be broken. Authentication of digitally signed information relies upon the integrity of the cryptography used. This will be compromised over time and digital signatures alone cannot therefore meet the requirements for reliable long-term evidence
- At some unknown time in the future, every digital certificate will expire or be revoked and will be published as being revoked or invalid; leaving all the data that was signed using that certificate in an unknown state
- Most digital signatures rely on a series of certificates in a certification chain. Revocation of any one certificate in a chain means that a digital signature relying on any certificate in that chain cannot be validated
- Lack of Trusted Time. Digital signatures and Public Key Infrastructures do not include trusted time let alone time that can be validated at any point in the future. Digital Evidence however requires verifiable proof of the time and sequence of events



For viable evidence therefore, digital signatures are deficient as they can only assist in validating the “who” and the “what”, not the “when”, and can only do this while the whole certificate chain remains intact and valid. Digital signature systems are too complex for the layman to understand and validate. The legal profession has not generally accepted conventional PKI based digital signatures as evidence due to the complexities of implementation and understanding and, in particular, the difficulties of ensuring that digital signatures remain valid over any significant period: a is crucial requirement for reliable evidence

## Legal Features & Ramifications

### Evidence Seals™:

“Having reviewed the material available to me that explains the nature and function of the system, I am for these purposes of the opinion that the security aspect of the system with regard to the preservation of important data relating to provenance, security, accuracy and authenticity of the data that the system protects would be of significant advantage”  
J Riley Q.C



- Support Electronic Signature legislations, which are now explicitly recognised in most international law:
  - UK Electronic Communications Act 2000
  - European Directive 199/93/EC on a Community Framework for Electronic Signatures
  - US-ESIGN (Electronic Signatures in Global and National Commerce) Act 2000
- Support the standard code of practice for legal admissibility PD0008: "A code of practice for Legal Admissibility and Evidential Weight of Information Stored Electronically"
- Support the standard code of practice for legal admissibility: PD5000 "An International Code of Practice for Electronic Documents and e-Business Transaction"
- Support the authenticating documentary evidence in line with section 8 of the UK Civil Evidence Act 1995

# Technical Overview

Evidence Seals™ provide irrefutable and durable evidence of the Who, What, When of any document, business record or data object.

- Evidence Seals™ preserve the authenticated identity and context of the user at the time the data is Sealed
- Evidence Seals™ prove the integrity of data by ensuring that any modification to the data can be detected
- Evidence Seals™ bind and preserve the time of Seal creation with the sealed data, synchronised with one or more trusted time sources
- Evidence Seals™ allow protected data to be independently validated, to the satisfaction of regulators or the courts, at any time in the future



Once sealed, protected data cannot be repudiated

The applicability of Evidence Seals™ is virtually unlimited. In an increasingly regulated and scrutinized world, wherever data in electronic form, such as documents, business records or transactions, may need to be presented as evidence, Evidence Seals™ will prove the authenticity, provenance and timing of the data. Once sealed, records can be held for as long as required and independently validated at any time providing the durability and certainty normally only associated with paper documents.

**Non-repudiation** is the ability to ensure that a party to a contract or a communication cannot deny the validity of the contract or of a communication that they originated. In today's global Internet economy, where face-to-face agreements are often not possible, businesses and regulators are increasingly aware of the vital need for electronic non-repudiation.

## Sealing Operation

### *Detail*



Evident Seals™ client software produces an electronic signed hash of application (user) data to be sealed; a hash is a mathematical digest of the data using a one-way function, such as SHA-1 or SHA-256. The hash is then electronically signed using a cryptographic algorithm, the keys being automatically generated and managed by the evidence management systems. This signed hash, together with application specific evidence Meta data, such as information about the user and the requesting service, is sent to an Evidence Manager™ via an encrypted link as seal creation request.

On receiving a seal creation request, the Evidence Manager™ checks the requesting service client is known and authorised. If the Seal request is valid, Evidence Manager™ obtains the current time from one or more trusted time sources and binds all the evidence data together to create the Evidence Seal™. The seal itself is stored on one or more archives which are also sealed, to create Evidence Sealed Archives, and a copy of the Evidence Seal™ is sent back to the requesting service.

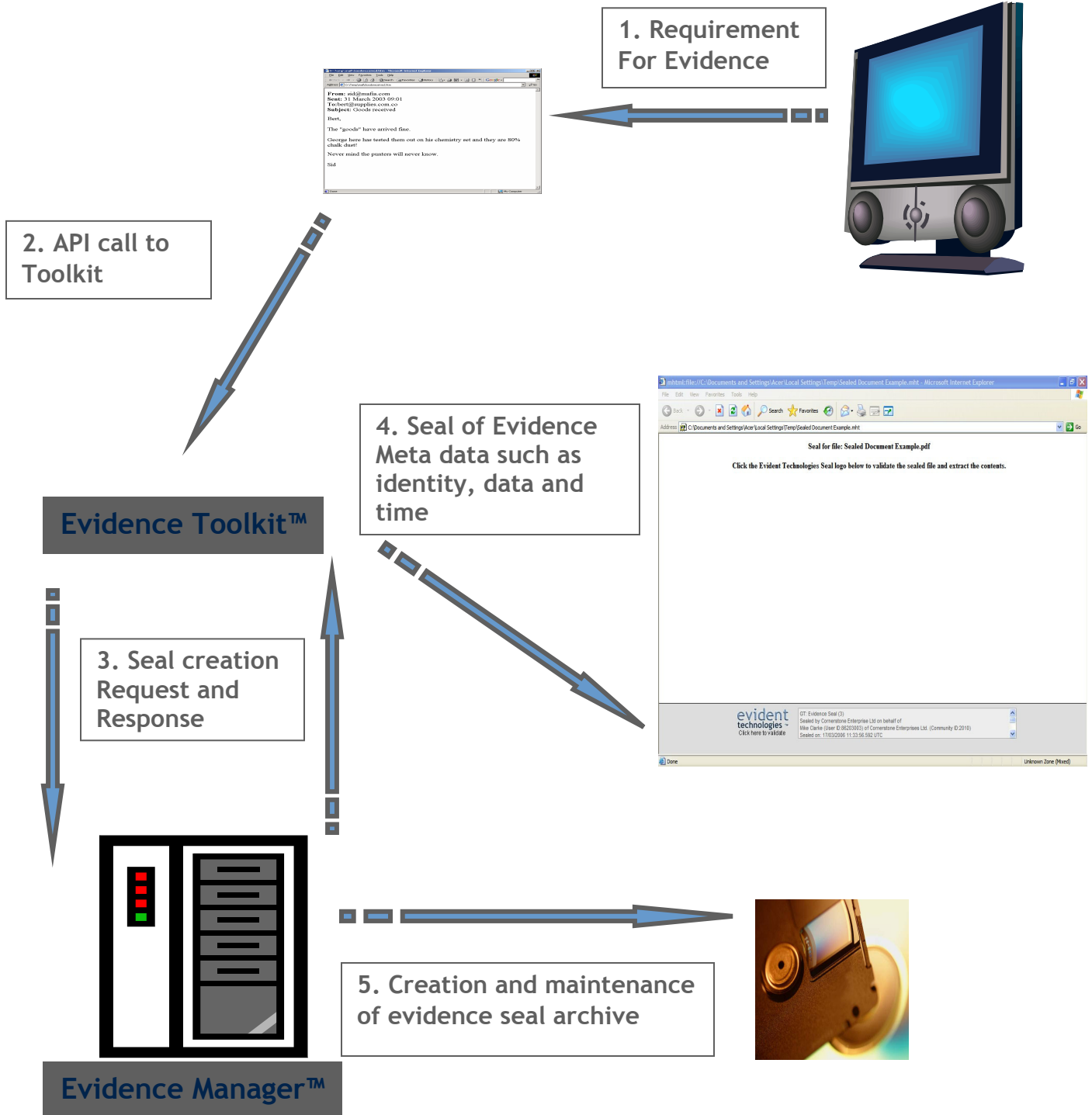
The functions of the sealing authority are implemented within a secure, tamper proof server system - the Evidence Manager™. with a FIPS 140 compliant cryptographic module and secure links to one or more trusted time sources. The architecture of the Evidence Manager allows for full redundancy.

The Seal proves that all the sealed evidence Meta data was authentic at the time the seal was created. As a minimum the sealed evidence Meta data includes: the application (user) data identified by the signed hash, authenticated information about the seal requesting entity (user), a trusted time mark and application specific data that is needed for long term evidence purposes.

Seals and the data they protect are archived for as long as the data and its evidence are required to be maintained. Evidence Seals™ do not depend on any particular encryption algorithm, strength or key length. A design premise of Evidence Seals™ is that, over time, all encryption mechanisms are vulnerable. The Seal Archives are therefore periodically re-sealed using latest techniques and client software hashing techniques are updated.

Seal archives do not compromise the confidentiality of business data, as only one-way hashes of data are maintained by the Evidence Seal™.

# Sealing Operation Graphic



## The Evidence Seal™

The format of an Evidence Seal™ uses standard data structures, including XML, HTML and MHTML. The electronic signatures within the Evidence Seals™ use standard binary signature formats including RFC 2630 and RFC 3161.

Evidence: Transaction Seal (1)  
Sealed by Evident Group Ltd on  
behalf of Nick Pope (User  
ID:10882) of Evident Group  
(Community ID:10028) Sealed on:  
20/01/2006 16:33:29.469 UTC

MIIDUAYJKoZIhvcNAQcCoIIDQTCCA  
zOCAQMxCzAJBgUrDgMCGGUAMIIB  
MgYLKoZIhvcNAQkQAQSGggEhBIIB  
HTCCARkCAQEGCisGAQQBhFkAw  
EwHzAHBgUrDgMCGGU.....

Computers do not go to court - people do. Format data needed for computers is, however, not in a form readily understood by humans. Therefore, the presentation of evidence metadata in the seal is flexible and can be presented for simple human understanding. For example using a plain language header describing the Seal in words that are readily understood. Illustrated on the side is a binary seal with a plain language header.

An Evidence Seal™ is typically less than 3K in size. Variability is determined by the optional application (user) defined evidence metadata that is also included in the Seal.

An Evidence Seal™ can be stand alone files or may be integrated with user data using text, XML or through use of the MHTML aggregate multi-media document structure, standardized in RFC 2557.

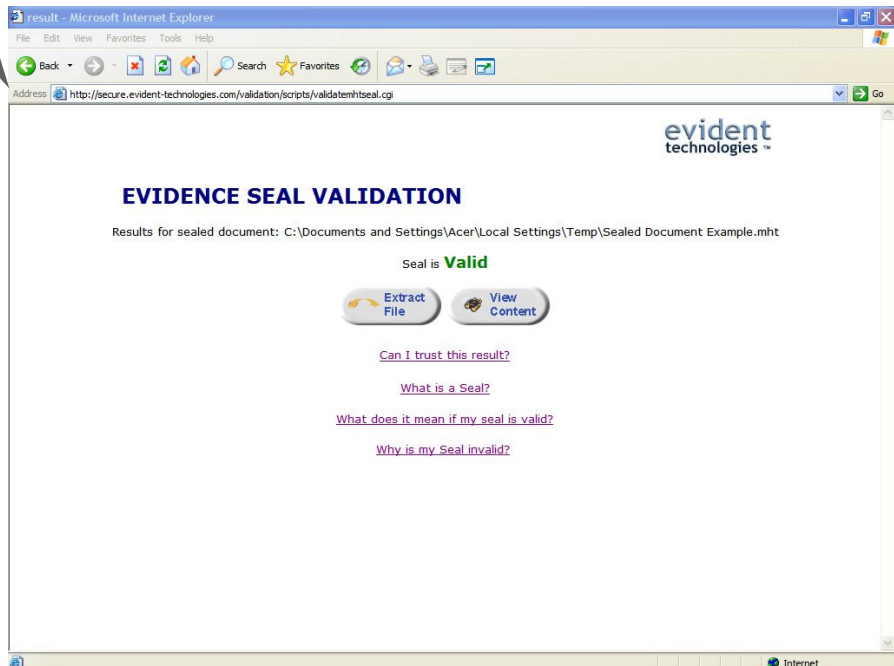
Using the flexibility of the MHTML structure, it is possible to display a Seal's plain language header in a manner that clearly associates it with the sealed object. The MHTML structure can also be used to handle a wide range of document types including Microsoft Word®, Web pages, images or video clips. Sealed objects in MHTML can be displayed and validated by any capable web browser, such as Internet Explorer, without the need for special software.

Seal creation and validation can also be integrated into any business application and presented to, or hidden from, the user as dictated by business process and requirements.

# A Sealed Document



Single 'Click'  
Instant Validation  
or 'Automatic' on  
document opening



## Evidence Manager™

An Evidence Manager™ is a tamper proof network appliance that creates and stores Evidence Seals™.

A specialised unit supplied as a pre-configured hardware and software package. It is a standard, rack mountable unit requiring no user organization intervention. The unit may be placed on the corporate intranet or accessed over the Internet to support any application requiring the protection of Evidential Seals™. All Evidence Manager™ accesses are protected using authentication checks and SSL/TLS transmission security.



An Evidence Manager™ creates a log of all the Seals it creates. This log is itself sealed and can be lodged at any suitable storage facility including a trusted third party to provide additional assurance and independent validation for sealed data.

Employing a FIPS 140-1 level 3 compliant hardware security module. All time and signing processes are performed within the hardware security module boundary to provide the highest levels of integrity. The hardware employed supports multiple cryptographic algorithms, is able to resist attempted attacks and to perform processing securely.

Also employing a trusted time calibration and audit service, this ensures that Evidence Manager™ time is consistently updated and traceable to officially recognised UTC time sources.

The Evidence Manager™ sealing service provides the equivalent of conventional PKI certification but without the hassle of PKI management, plus auditable, trusted time-stamps and a real time revocation-status capability, within a single, integrated service.

# Applications

## *Evidence Toolkit™*

Evidence Toolkit™ provides a set of API calls that allow any business application or service to become “evidence enabled”. Evidence Toolkit™ supports a wide range of software environments and provides all the tools necessary to simply add Evidence Seals™ to an application.

Evidence Toolkit™ communicates with one or more Evidence Managers™ to fulfill Evidence Seal™ requests. Each toolkit and the services that it supports are registered and known to their Evidence Manager(s)™. Evidence Toolkit™ allows application (user) defined metadata to be presented for inclusion in Evidence Seals™.

Programmatically, all that is required is to present the data to be sealed to a program interface, and Evidence Toolkit™ passes back the Evidence Seal™. The seal can be handled as a simple text string, as a MIME/HTML multi-media document, or as an XML element.

Evidence Toolkit™ similarly allows data to be validated by a simple call from your application. In addition or alternatively, users can independently validate sealed data through web browser.

The toolkit provides all the tools necessary to add Evidence Seals™ to an application.

Together Evidence Toolkit™ and Evidence Manager™ -

- Can certify users identities without the need for an expensive Public Key Infrastructure
- Can work with existing or new third party authentication system, extending the proof of identification to have long term evidential properties
- Automatically provide all necessary keys and passwords
- Ensure that only valid users create Evidence Seals
- Maintain logs of sealing data, time synchronisation events and all other data needed to corroborate evidence
- Maintain the privacy of user data



## Applications

### *Packaged solutions*

In addition to Evidence Toolkit™, a portfolio of packaged application solutions is available providing the protection of Evidence Seals™ to selected environments without the need for programming effort.

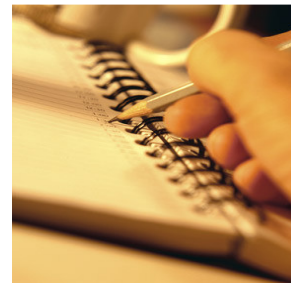
The portfolio includes -

- Evident Desktop File Sealer™: a “drag and drop” Windows® desktop application providing evidence for any file type
- Evident Mail™: implemented within an MTA, provides evidence of original e-mail content including attached files for inbound and outbound mail
- Evident Office™: A Microsoft Office® application providing toolbar generated evidence of any Word®, Excel® or PowerPoint® file

Solutions are also available to provide evidence for Voice and Video records and of Web site content.

## In Summary

- Evidence Seals™ provide irrefutable and durable evidence of digital activity in a cost effective solution that is simple to install and to use without disruption to business applications
- At a minimum, the Seal provides evidence of Who, What and When, in a manner that cannot be repudiated
- The Seal provides evidence of application or user specific information using the Evidence Metadata
- Business confidence is maximised and risk minimised by providing strong evidence which is human understandable, can be independently validated and lasts for long periods of time
- Evidence Seals™ provide long-term evidence without the need to rely on paper originals or copies. While independent, 3<sup>rd</sup> party validation is supported, protected data need never leave the business, maintaining and enhancing confidentiality
- Seals secure the business process without imposing change on the way business is done. The disruption and excessive management overheads normally associated with a Public Key Infrastructure, are avoided



## Evidence Seals <sup>™</sup> *the Designers*

John Ross and Nick Pope are two leading security technology experts who have been active in developments of security protocols from the earliest public key infrastructure (PKI) standards to recent work on policy criteria for assessing security infrastructures, and have been architects for some key national security infrastructures

- Nick sits on the EU Directive Panel for Digital Signatures, consults to the American Bar Association and co-chairs the Oasis committee
- John consults to the UK Governments E-Envoy & Cabinet Offices
- Together they have over 30 years experience in providing systems for the UK government, MoD, NATO, European Commission, BT, SWIFT and others

