

Orion Systems' Tamper-proof, Fraud-Resistant, and Non-Repudiation Security White Paper

White Paper

Updated: Spring 2011

<http://www.orisys.com/>



United States Patent 6,745,936, 7,246,097



CONTENTS

ORION SYSTEMS SECURITY WHITE PAPER.....	1
CONTENTS	2
EXECUTIVE OVERVIEW	3
Introduction	3
ORION'S BROAD AND FUNDAMENTAL PATENT.....	4
Tamper-Proof and Fraud-Resistant : Broad Patent Overview	4
ORION'S IMPLEMENTATION	8
Tamper-Proof, Fraud-Resistant,Non-Repudiation: Implementation	8
CONCLUSION	10

This paper address the security offered in Orion Systems' eSigner Software and Patent Licensing Offerings. Orion Systems is a leading provider of electronic signature and other biometric software solutions, and has developed a deep understanding of the requirements for legal enforceability of electronic signatures and contracts, as well as a thorough knowledge of the transaction, business and other processes that direct it. Through continuing research, Orion has become an expert authority on using and securing electronic records of all types - legally binding contracts, leases, loans, HIPAA forms, and personal information documents.

In this paper, we identify and define each of the security components that make up the tamper-proof, fraud-resistant, and non-repudiation nature of our technology comprised in all of our software and patent licensing offerings.

The first section is dedicated to Orion's patent describing the important security elements of the patent. The second section is dedicated to Orion's security technology and its implementation.

For more information on Orion's Solutions, please visit our website at <http://www.orisys.com/>

Tamper-Proof and Fraud-Resistant : Broad Patent Overview

The nature of Orion's Highly Secure technology is based upon our fundamental patent number (#6,745,936) filed in 1996 entitled, **Method and apparatus for generating secure endorsed transactions**. Orion retains the services of the prestigious law firm of Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P. Based in Washington, DC, Finnegan, Henderson, et. al. has over 300 partners, specializing in IP with a world wide presence.

The abstract our of patent reads: "To ensure the data corresponding to transactions has not been altered, a method and system are provided for generating secure endorsed transactions having transaction data representative of transactions and unique identifiers corresponding to parties endorsing the transactions. After receiving input, including transaction data and unique identifiers, unique codes are generated from the transaction data and unique identifiers. The unique codes constitute secure endorsements of the transaction data by the parties corresponding to the unique identifiers."

There are several key components identified in the abstract. They are 1) transaction data, 2) unique identifiers corresponding to the endorsing parties and 3) unique codes. The transaction data is the contract, receipt or document being signed. The unique identifiers are the biometrics that uniquely identifies the signer(s). The unique codes are derived directly from the combination of transaction data and unique identifiers. Let's explore each of the components in greater detail, considering how they relate to the patent and our technology.

Transaction Data

The transaction data can be any type of data. It is non-specific. Some examples of transaction data include commerce entities such as credit card purchases, equipment and vehicle rentals, and mortgage loans. Other examples of transaction data include business forms requiring approvals, such as purchase orders, work requisitions, and hiring forms. Still other types of transaction data include medical or insurance forms such as HIPAA forms or Insurance enrollment forms.

Transaction data is made up of both the content and the look and feel of the document. The content is simply the composition that includes the language and the information within the body of the document. The look and feel is the display component that includes formatting instructions such as font specification, point and type elements, and other specifics that control the look of the document to the human eye.

Orion's patent includes all types of transaction data.

Unique Human Identifiers

Unique human identifiers are more commonly referred to as biometrics. There are several different types of biometric capture devices capable of reading or scanning an individual's signature, fingerprint, retina, face, and voice. Although these are the more common biometrics that are capturable with today's technology, a unique human identifier is not specific to just this list. It includes a uniquely identifying mark or element of a human being. As technology progresses, there is sure to be other interesting biometric capture devices developed. ***Orion's patent includes all possible biometrics.***

Unique Codes

Unique codes are generated from the transaction data and unique identifiers. The transaction data and unique identifiers are combined, and then computed to a unique code, shorter yet representing the entire combination. There are a few methods of computing unique codes: XOR, or check summing the data, and Hashing Functions (also referred to as Message Digesting) are the most common. ***Orion's patent includes all possible Unique Code Algorithms.***

Claim One

The first claim of our patent reads "A secure endorsed transaction system, comprising: an encoder that generates a unique code from input data comprising transaction data, a human identifier that uniquely identifies a human being, and a second key of an asymmetrical key pair that includes the second key and a corresponding first key; a digital signature processor that generates a digital signature by encrypting the unique code using the first key; a formatter that formats a secure endorsed transaction using the digital signature and the input data; and a verifier that verifies integrity of the secure endorsed transaction by, as a function of the secure endorsed transaction, comparing a stored unique code derived by decrypting the digital signature using the second key with a computed unique code derived from the second key, the human identifier, and the transaction data."

There are several key components identified in claim 1. They are 1) an encoder, 2) an asymmetrical two key cryptosystem, 3) a formatter, and 4) a verifier. Let's explore each of the components in greater detail, considering how they relate to the patent and our technology.

Encoder

The encoder encodes the transaction data with the biometric, producing a unique code that represents the whole. A unique code is a shorter value than the whole, yet represents the entire whole uniquely. Examples of encoders are XOR check summing and Hashing. Hashing (MD5 or SHA) is the most common and powerful method of encoding, as it contains the property of creating a hashing code that is computationally difficult to reproduce with dissimilar input. ***Orion's patent encompasses all possible encoding schemes.***

Asymmetrical Two-Key Cryptosystem

The Asymmetrical Two-Key Cryptosystem employs two keys (one public and one private) that are not the same (they are asymmetrical). Examples of these types of systems are RSA's Public Key System or DSA (US Government's Digital Signature Algorithm). After the encoder produces a unique code, the code is encrypted using one of the two keys, producing what is commonly referred to as a digital signature. ***Orion's patent encompasses all possible Asymmetrical Two-Key Cryptosystems.***

One of the benefits of using such a system is that the second key can be used to decode the digital signature without compromising the security. What this essentially means is that the Public Key can be made available for non-repudiation, verification, and authentication without exposing the security, as the Private Key (the key used in the encryption) cannot be derived from the Public Key.

Formatter

Once a digital signature is produced, the digital signature, original transaction data and biometrics are formatted so as to be easily accessible. By formatting all of these components together, one can move them to a database for archival and easy access for verification.

Verifier

Once all of the pieces are formatted and stored, a verifier is available that allows one to access the formatted content and verify its integrity. Verification is accomplished by extracting the transaction data and biometrics, calculating a new unique code from them and comparing the new unique code with the formatted code in the digital signature. If the codes are the same, then the transaction data and biometrics are verified as unchanged. If there is a difference between the unique codes, then a change occurred in the formatted transaction data or biometrics, and the verification fails. The act of verification when used with hashing codes and digital signatures is more commonly referred to as nonrepudiation.

Section Summary

In conclusion, Orion's patent is extremely broad and fundamental. It specifies no single type of transaction, unique human identifier, unique code algorithms, or Asymmetrical Two Key Cryptosystems and provides the basis of creating a highly secure endorsed transaction that is tamper-proof, fraud-resistant, and non-repudiatable.

Orion Systems' eSigner security system is based on Orion's patent #6,745,936 entitled **Method and apparatus for generating secure endorsed transactions**. As stated in the previous section, the first claim reads: "A secure endorsed transaction system, comprising: an encoder that generates a unique code from input data comprising transaction data, a human identifier that uniquely identifies a human being, and a second key of an asymmetrical key pair that includes the second key and a corresponding first key; a digital signature processor that generates a digital signature by encrypting the unique code using the first key; a formatter that formats a secure endorsed transaction using the digital signature and the input data; and a verifier that verifies integrity of the secure endorsed transaction by, as a function of the secure endorsed transaction, comparing a stored unique code derived by decrypting the digital signature using the second key with a computed unique code derived from the second key, the human identifier, and the transaction data."

The patent is very broad and doesn't specify a number of the key elements such as encoding schemes, biometrics, and asymmetrical two-key systems. As a patent, this is desirable, as all of the possible elements are encompassed within the body of our patent to provide our customers with the broadest protection possible. It is because of these broad claims that our patent is regarded as so fundamental.

The focus of this section is to convey the elemental details Orion has chosen to implement to provide the highest level of security possible.

The essence of our patent can be found in claim one. It lays out the key elements of the patent.

There are several key components identified in the claim 1. They are 1) an encoder 2) an asymmetrical two-key cryptosystem 3) a formatter and 4) a verifier. Let's explore each of the components in greater detail, considering how they relate to Orion's implementation.

Encoder

The first element is the encoder. The encoder is responsible for encoding the transaction data and the biometrics. Orion's software uses the latest and most powerful Hashing Algorithms available. As new and stronger Hashing Functions algorithms become available, Orion makes these available to our customers under terms of their maintenance contracts.

Asymmetrical Two-Key Cryptosystem

The next element is the Asymmetrical Two-Key Cryptosystems. This element is responsible for encrypting the hash code or message digest and creating the digital signature. Orion uses the Public Key cryptosystem. A private key is used to encrypt the hash code, and the public key is used to decrypt the hash code. Orion registers their keys with a third-party certification house. To give our customer's additional flexibility, Orion's gives customers the ability to use their own keys. These keys can be rolled as often as necessary without any change in our software.

Formatter

The next element is the formatter. Orion places all of the security elements (original transaction data, biometrics, public key, and digital signature) into a single file. This file is known as the .REC (or DOT REC) file. Other pieces of information are stored in the .REC file, including the time-stamps of when the transaction was created, the index and SQL search codes, and an audit trail. This is all of the information needed to verify and authenticate the transaction.

Verifier

The final element is the verifier. The verifier is responsible for authenticating the stored .REC file and to nonrepudiate the transaction. By using the stored public key, Orion retrieves the .REC file and decrypts the stored digital signature, then compares this with a re-calculated digital signature using the stored transaction data and biometric data. If the hash codes match, then the .REC is unaltered. If the hash codes don't match, then the .REC has been tampered with.

CONCLUSION

Orion Systems is a leading software developer of secure paperless solutions employing electronic signatures, fingerprints and other biometrics. Based on our fundamental patent, our software is the only solution that securely and irrefutably electronically binds your customer's or employee's biometrics to your document, creating a legally enforceable signed document. Our products, designed specifically to address key industry needs, can be viewed online at our website, www.orisys.com.

Orion Systems maintains a diverse portfolio of intellectual property (IP), including copyrights, trademarks, trade secrets, and patents. Like other technology providers, our technology is licensed by business entities worldwide, and we routinely apply to governments around the world to obtain additional patents on our inventions. A patent establishes ownership of an invention, enabling the patent owner to benefit commercially from investments in innovation. A patent is granted if government patent examiners conclude that an invention is a true innovation compared with existing technology. Orion Systems has been awarded United States patents, and our worldwide portfolio continues to grow. Parties interested in licensing Orion's IP are encouraged to contact our Intellectual Property and Licensing Group by submitting an online request.

If you have feedback about this document, please send e-mail to: sales@orisys.com.

Boston Office

15 New England Exec Park
Burlington, MA 01803

Austin Office

9600 Great Hills Trail
Suite 150W
Austin, TX 78759

Tel: 1-877-OrionSign (674-6674)
www.orisys.com

©Copyright 2011, Orion Systems, Inc. All rights reserved. Registered or unregistered trademarks in this document are property of their respective owners. The products in this document are protected by one or more patents, US. Patent number 6,745,936 and 7,246,097. Specifications subject to change without notice.