

**EXHIBIT C: THE '848 PATENT INVALIDITY CLAIM CHART**

U.S. Patent No. 5,872,848	Dziewit et al., U.S. Patent No. 5,031,214	Bisbee et al., U.S. Patent No. 5,748,738
<p>1. A method for authenticating an electronic document comprising the steps of:</p>	<p>Claim 1 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.</p> <p>Dziewit teaches a method for authenticating an electronic document. (See Col. 2:3-68 and Col. 12:44-57).</p>	<p>Claim 1 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.</p> <p>"System and Method for Electronic Transmission, Storage and Retrieval of Authenticated Documents." (Title).</p>
<p>[a.] generating a first digital signature of an originating party for said electronic document;</p>	<p>"In such a situation, it is typical to have all the parties collocated so the witnesses can attest to the <b>first party signing the document</b> by placing their signatures electronically on the document." (Col. 12:53-57)(emphasis added).</p> <p>"Once validation of the identification of all contracting parties is obtained, then the file 'document' is 'signed' by all the parties and the legal document has been executed electronically." (Col. 12:48-51).</p> <p>"The actual 'signing' or authenticating of the electronic document can be implemented as an additional password step utilizing personnel identity validation apparatus." (Col. 2:35-38).</p> <p>"The authentication of the document by the contracting parties consummates the execution of the document. The document authentication</p>	<p>"In the second step, the parties to the agreement execute their hand-written signatures on the document using the stylus pad. These signatures are captured and inserted in appropriate locations in the electronic document. After all parties have signed the document, the Transfer Agent certifies the completion of the document's execution by invoking his or her digital signature and appending his or her certificate, using the Token." (Col. 9:41-49).</p> <p>Bisbee teaches the use of digitized <i>electronic signatures</i> rather than <i>digital signatures</i>. However, the <i>electronic signature</i> genus includes the <i>digital signature</i> species. Moreover, both Bisbee and the '848 patent admit to the need for digital signatures to preserve the integrity of an electronic document. (Bisbee at Col. 2:11-61 and Col. 9:45-49; '848 patent at Col. 2:53-61). To better assure the integrity of an electronic document, one of skill in</p>

<p><b>U.S. Patent No. 5,872,848</b></p>	<p><b>Dziewit et al., U.S. Patent No. 5,031,214</b></p> <p>apparatus responds to the authentication operation by providing sufficient safeguards to insure that the contents of the file have not been modified or altered following the consummation of the multi-party contract single party document without the alteration being detectable. This is typically accomplished by the generation of a 'digital signature' that 'fingerprints' the document such that not even a single bit of the document can be altered without this change being reflected in the digital signature." (Col. 2:47-58).</p> <p>Dziewit is ambiguous as to whether the co-located parties sign the electronic document with <i>digital signatures</i> or <i>electronic signatures</i> (such as a <i>digitized signature</i>). To the extent the parties use <i>digital signatures</i>, the <i>digital signatures</i> limitation of claim 1 is explicitly taught by Dziewit. If the Dziewit signatures are <i>electronic signatures</i>, the <i>digital signatures</i> limitation of claim 1 is rendered obvious by Dziewit. The definition of <i>electronic signatures</i> includes <i>digital signatures</i>. Both Dziewit and the '848 patent admit to the need for digital signatures to preserve the integrity of an electronic document. (Dziewit at Col. 12:62-67; '848 patent at Col. 2:53-61). To better assure the integrity of an electronic document, one of skill in the art would have been motivated to use <i>digital</i></p>	<p><b>Bisbee et al., U.S. Patent No. 5,748,738</b></p>	<p>the art would have been motivated to use <i>digital signatures</i> in place of the digitized <i>electronic signatures</i> of Bisbee.</p>
---	---	--	---

<p><b>U.S. Patent No. 5,872,848</b></p>	<p><b>Dziewit et al., U.S. Patent No. 5,031,214</b> <i>signatures in place of the electronic signatures of the co-located parties taught by Dziewit.</i></p>	<p><b>Bisbee et al., U.S. Patent No. 5,748,738</b></p>
<p>[b.] generating an identification envelope comprising a verifying statement for said electronic document, said verifying statement comprising a statement of a verifying party indicating that said verifying party witnessed execution of said first digital signature by said originating party;</p>	<p>"In such a situation, it is typical to have all the parties collocated so the witnesses can attest to the first party signing the document by placing their signatures electronically on the document." (Col. 12:53-57)(emphasis added).</p> <p>Dziewit does not explicitly specify the existence of a <i>verifying statement</i>; however, the presence of such a statement must inherently exist since the witnesses attest to witnessing the signing of the electronic document. This "attestation" is a <i>verifying statement</i>. Moreover, the '848 patent itself admits to the routine nature of a <i>verifying statement</i> in prior art Notarial practice. (Col. 1:15-22).</p> <p>Dziewit does not teach the creation of an <i>identification envelope</i>, but the '848 patent itself admits to such statements being routine in standard Notarial practice. Specifically, in its description of the prior art, the '848 patent teaches: "For certain transactions, authentication of a handwritten signature, for example by a licensed public official such as a notary, is required. Authentication of a signature by a notary requires a personal appearance before the notary. The notary</p>	<p>"After all parties have signed the document, the Transfer Agent certifies the completion of the document's execution by invoking his or her digital signature and appending his or her certificate, using the Token." (Col. 9:41-49)(emphasis added).</p> <p>"The DAS also would permit a 'Notary Public' type of secondary support function. This would permit a third party present at the document's execution to also have a cryptographic card which would "seal" the transaction for further verification that the parties executing or sealing the document to be signed were in fact the proper parties. This additional notary function is not required, but would assist in the further authentication of the identities of the parties." (Col. 8:55-62). (This teaching also exists in the '738 patent considered during prosecution of the Romney patent).</p> <p>Bisbee does not teach the creation of an <i>identification envelope</i>, but the '848 patent itself admits to such statements being routine in standard Notarial practice. Specifically, in its description of the prior art, the '848 patent teaches: "For certain transactions, authentication of a handwritten</p>

<p><b>U.S. Patent No. 5,872,848</b></p>	<p><b>Dziewit et al., U.S. Patent No. 5,031,214</b></p> <p>personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature, and <b>affixes a notary statement and seal to the signed document.</b>" (Col. 1:15-22)(emphasis added). Thus, it would have been obvious to one of skill in the art to include an <i>identification envelope</i> when the co-located witnessing party of Dziewit is a Notary.</p>	<p><b>Bisbee et al., U.S. Patent No. 5,748,738</b></p> <p>signature, for example by a licensed public official such as a notary, is required. Authentication of a signature by a notary requires a personal appearance before the notary. The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature, and <b>affixes a notary statement and seal to the signed document.</b>" (Col. 1:15-22)(emphasis added). Thus, it would have been obvious to one of skill in the art to include an <i>identification envelope</i> in the system of Bisbee.</p>
<p>[c.] generating a second digital signature of said verifying party for said electronic document and for said identification envelope.</p>	<p>"In such a situation, it is typical to have all the parties collocated so the witnesses can attest to the first party signing the document <b>by placing their signatures electronically on the document.</b>" (Col. 12:53-57)(emphasis added).  See Claim 1a.</p>	<p>"In the second step, the parties to the agreement execute their hand-written signatures on the document using the stylus pad. These signatures are captured and inserted in appropriate locations in the electronic document. After all parties have signed the document, the Transfer Agent certifies the completion of the document's execution by invoking his or her digital signature and appending his or her certificate, using the Token." (Col. 9:41-49).  See Claim 1a.</p>
<p>2. The method of claim 1 further comprising the step of verifying said first digital</p>	<p>Claim 2 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.</p>	<p>Claim 2 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.</p>

<p><b>U.S. Patent No. 5,872,848</b></p> <p>signature prior to generating said identification envelope for said electronic document.</p>	<p><b>Dziewit et al., U.S. Patent No. 5,031,214</b></p> <p>The '848 patent admits that routine Notarial practice involves the verification of the signature. (Col. 1:15-22). It would have been obvious to include this step in the Dziewit method.</p>	<p><b>Bisbee et al., U.S. Patent No. 5,748,738</b></p> <p>The '848 patent admits that routine Notarial practice involves the verification of the signature. (Col. 1:15-22). It would have been obvious to include this step in the Bisbee method.</p>
<p>3. The method of claim 1 wherein said identification envelope comprises biometric data of said originating party.</p>	<p>Claim 3 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.</p> <p>"In either case, the personnel identification process is initiated at step 321 by the individual (first party) to be bound by the file "document" assenting to the form and content of the file "document" as is presently stored in the document authentication software 143. The assent is obtained by personnel identification process 205 polling the individual (first party) to obtain initial confirmation that authentication is appropriate. At step 322, personnel identification process 205 enables and scans a sensor (ex. device 142) associated with the first party. The sensors, as described above, can be as elemental as a prompt to the terminal associated with the selected party to enter a password that is theoretically known only to the selected party. The accuracy of personnel identity validation can be improved by the addition of various peripheral devices 142, 141 that measure some immutable physical characteristic of the party. These devices include fingerprint scanners, voiceprint identifiers, retina scanners, etc." (Col. 12:8-26).</p>	<p>Claim 3 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.</p> <p>"In an additional aspect of Applicant's invention, the public/private key is only effective when it is used in conjunction with a certificate and personal identification information such as the recipient's biometric information (e.g., retina-, finger-, and voice-prints) or a personal identification number (PIN) that is assigned to the recipient of the card by the Certification Authority and that may be delivered separate from the originator's card." (Col. 4:61 - Col. 5:1).</p> <p>"The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature, and affixes a notary statement and seal to the signed document." ('848 at Col. 1:18-22).</p> <p>Thus, the '848 patent admits that prior art Notarial processes involve the inspection of identity documents. Bisbee teaches the use of biometric data as a means of using a digital signature. To</p>

<p><b>U.S. Patent No. 5,872,848</b></p>	<p><b>Dziewit et al., U.S. Patent No. 5,031,214</b></p> <p>The '848 patent teaches: "The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature, and affixes a notary statement and seal to the signed document." ('848 at Col. 1:18-22).</p> <p>Thus, the '848 patent admits that prior art Notarial processes involve the inspection of identity documents. Dziewit teaches the use of biometric data for identification purposes. To ensure proper identification of the originating party, it would have been obvious to modify Dziewit to record the biometric data and to include that information in the identification envelope.</p>	<p><b>Bisbee et al., U.S. Patent No. 5,748,738</b></p> <p>ensure proper identification of the originating party, it would have been obvious to modify Bisbee to record the biometric data to identify the originating party, and to include that information in the identification envelope.</p>
<p>4. The method of claim 3 wherein said biometric data comprises a digitized fingerprint of said originating party.</p>	<p>Claim 4 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.</p> <p>See Claim 3.</p> <p>"These devices include <b>fingerprint scanners</b>, voiceprint identifiers, retina scanners, etc." (Col. 12:24-26)(emphasis added).</p>	<p>Claim 4 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.</p> <p>See Claim 3.</p> <p>"In an additional aspect of Applicant's invention, the public/private key is only effective when it is used in conjunction with a certificate and personal identification information such as the recipient's biometric information (e.g., retina-, <b>finger</b>-, and <b>voice-prints</b>) or a personal identification number (PIN) that is assigned to the recipient of the card by the Certification Authority and that may be</p>

U.S. Patent No. 5,872,848	Dziewit et al., U.S. Patent No. 5,031,214	Bisbee et al., U.S. Patent No. 5,748,738
<p>5. The method of claim 1 wherein said identification envelope comprises a public key of said originating party.</p>	<p>Claim 5 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.</p> <p>"A more secure and complex system that minimizes the possibility of fraud by the contracting parties is the RSA Public Key Cryptosystem. This system uses two encryption keys. A "private key" is used by the document sender to scramble the data while a "public key", known to the document recipient, is used to decode the received document." (Col. 7:6-12).</p> <p>The '848 patent teaches that a party "freely distributes its public key." (Col. 2:17-18). Thus, it would have been obvious to include a copy of the originating parties' public key in the identification envelope.</p>	<p>delivered separate from the originator's card." (Col. 4:61 - Col. 5:1)(emphasis added).</p> <p>Claim 5 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.</p> <p>"In one aspect of Applicant's invention, a method of authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes." (Col. 30-37).</p> <p>The '848 patent teaches that a party "freely distributes its public key." (Col. 2:17-18). Thus, it would have been obvious to include a copy of the originating parties public key in the identification envelope.</p>
<p>6. The method of claim 1 wherein said identification envelope comprises a digital certificate of said originating party.</p>	<p>Claim 6 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.</p> <p>"Digital encryption, digital message digests, digital signatures, and digital certificates are some of the existing cryptographic tools that are used in the</p>	<p>Claim 6 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.</p> <p>"In one aspect of Applicant's invention, a method of authenticating an electronic document comprises the steps of: signing the electronic document with</p>

<p><b>U.S. Patent No. 5,872,848</b></p>	<p><b>Dziewit et al., U.S. Patent No. 5,031,214</b></p> <p>present invention to address this need." ('848 at Col. 1:46-49). "Digital signatures and digital certificates have been devised to address some of the uncertainties inherent in public key cryptography." ('848 at Col. 2:53-55). "Digital certificates are intended to provide a level of assurance as to the identity of the holder of the private key corresponding to a particular public key. The issuers of digital certificates are called certification authorities. A digital certificate constitutes a certification by a certification authority that a particular public key is the public key of a particular entity, and that this entity is the holder of the corresponding private key." ('848 at Col. 3:32-40). "The authenticity of a digital certificate is tested by verifying the certification authority's digital signature using the certification authority's public key." ('848 at Col. 3:61-63). "The digital certificate may be appended to an electronic document, or the recipient of an electronic document may obtain a copy of the certificate from the issuing certification authority or other certificate repository." ('848 at Col. 4:10-14).</p> <p>The '848 patent admits that the use of digital certificates to link a party to a digital signature was common in the prior art. Thus, it would have been obvious to include a digital certificate in the</p>
<p><b>Bisbee et al., U.S. Patent No. 5,748,738</b></p>	<p>a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes." (Col. Col. 3:3-10).</p> <p>"Issuance by the Certification Authority of a digitally signed certificate ensures the verifiability of the identity of each transmitter of a digitally signed or encrypted document." (Col. 5:15-17).</p> <p>Bisbee teaches the step of appending the digital certificate to an electronic document. It would have been obvious to include the digital certificate in the "identification envelope".</p>



U.S. Patent No. 5,872,848	Dziewit et al., U.S. Patent No. 5,031,214 method of Dziewit to verify ownership of the private/public key pair associated with the digital signature.	Bisbee et al., U.S. Patent No. 5,748,738
7. The method of claim 1 wherein said identification envelope comprises a digital certificate of said verifying party.	Claim 7 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.  See Claim 6.	Claim 7 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.  See Claim 6.
8. The method of claim 1 further comprising the step of appending indicators to said electronic document for delineating said identification envelope.	Claim 8 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent and U.S.P. 5,005,200.  The technique of "appending indicators" to an electronic document to delineate various sections of the document, such as "main text" and "digital signature is notoriously old. See, for example, Figure 8 of U.S.P. 5,005,200. It would have been obvious to include in the Dziewit method the step of appending indicators to delineate the identification from the signed document.	Claim 8 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent and U.S.P. 5,005,200.  The technique of "appending indicators" to an electronic document to delineate various sections of the document, such as "main text" and "digital signature is notoriously old. See, for example, Figure 8 of U.S.P. 5,005,200. It would have been obvious to include in the Bisbee method the step of appending indicators to delineate the identification from the signed document.
9. The method of claim 1 wherein said identification envelope comprises information identifying materials used by said verifying party to verify the	Claim 9 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.  "The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature,	Claim 9 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.  "The notary personally witnesses the execution of the signature, inspects identity documents to verify the identity of the person executing the signature,

<p><b>U.S. Patent No. 5,872,848</b></p> <p>identity of said originating party.</p>	<p><b>Dziewit et al., U.S. Patent No. 5,031,214</b></p> <p>and affixes a notary statement and seal to the signed document." ('848 at Col. 1:18-22).</p> <p>The '848 patent admits that prior art Notarial processes involve the inspection of identity documents. It would have obvious to include in the identification envelope information identifying which documents were inspected.</p>	<p><b>Bisbee et al., U.S. Patent No. 5,748,738</b></p> <p>and affixes a notary statement and seal to the signed document." ('848 at Col. 1:18-22).</p> <p>The '848 patent admits that prior art Notarial processes involve the inspection of identity documents. It would have obvious to include in the identification envelope information identifying which documents were inspected.</p>
<p>10. The method of claim 1 wherein said identification envelope is computer encoded.</p>	<p>Claim 10 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.</p> <p>The '848 provides limited explanation for what is meant by "computer encoded". In fact, the only mention of the term, outside the claims, is: "An authenticator statement may be in a human language or may be computer encoded." (Col. 9:27-28). Non-human language documents are notoriously old in the field of electronic documents -- in fact, all electronic documents are preserved as digital data in a non-human-readable format. Thus, it would have been obvious to computer encode the identification.</p>	<p>Claim 10 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.</p> <p>The '848 provides limited explanation for what is meant by "computer encoded". In fact, the only mention of the term, outside the claims, is: "An authenticator statement may be in a human language or may be computer encoded." (Col. 9:27-28). Non-human language documents are notoriously old in the field of electronic documents -- in fact, all electronic documents are preserved as digital data in a non-human-readable format. Thus, it would have been obvious to computer encode the identification.</p>
<p>11. A program storage device readable by a machine, tangibly embodying a program of instructions executable by</p>	<p>Claim 11 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.</p> <p>See Claim 1.</p>	<p>Claim 11 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.</p> <p>See Claim 1.</p>

U.S. Patent No. 5,872,848	Dziewit et al., U.S. Patent No. 5,031,214	Bisbee et al., U.S. Patent No. 5,748,738
the machine to perform a method for authenticating an electronic document, said method comprising the steps of:		
[a.] generating a first digital signature of an originating party for said electronic document;	See Claim 1a.	See Claim 1a.
[b.] generating an identification envelope comprising a verifying statement for said electronic document, said verifying statement comprising a verifying party indicating that said verifying party witnessed execution of said first digital signature by said originating party;	See Claim 1b.	See Claim 1b.
[c.] generating a second digital signature of said verifying party for said electronic document and for said identification envelope.	See Claim 1c.	See Claim 1c.

<b>U.S. Patent No. 5,872,848</b>	<b>Dziewit et al., U.S. Patent No. 5,031,214</b>	<b>Bisbee et al., U.S. Patent No. 5,748,738</b>
12. The program storage device of claim 11 wherein said method further comprises the step of verifying said first digital signature prior to generating said identification envelope for said electronic document.	Claim 12 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.  See Claim 2.	Claim 12 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.  See Claim 2.
13. The program storage device of claim 11 wherein said identification envelope comprises biometric data of said originating party.	Claim 13 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.  See Claim 3.	Claim 13 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.  See Claim 3.
14. The program storage device of claim 13 wherein said biometric data comprises a digitized fingerprint of said originating party.	Claim 14 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.  See Claim 4.	Claim 14 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.  See Claim 4.
15. The program storage device of claim 11 wherein said identification envelope comprises a public key of said originating party.	Claim 15 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.  See Claim 5.	Claim 15 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.  See Claim 5.
16. The program storage	Claim 16 is invalid as being obvious over Dziewit	Claim 16 is invalid as being obvious over Bisbee in

<p><b>U.S. Patent No. 5,872,848</b></p> <p>device of claim 11 wherein said identification envelope comprises a digital certificate of said originating party.</p>	<p><b>Dziewit et al., U.S. Patent No. 5,031,214</b></p> <p>in view of the prior art admitted by the '848 patent.</p> <p>See Claim 6.</p>	<p><b>Bisbee et al., U.S. Patent No. 5,748,738</b></p> <p>view of the prior art admitted by the '848 patent.</p> <p>See Claim 6.</p>
<p>17. The program storage device of claim 11 wherein said identification envelope comprises a digital certificate of said verifying party.</p>	<p>Claim 17 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.</p> <p>See Claim 7.</p>	<p>Claim 17 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.</p> <p>See Claim 7.</p>
<p>18. The program storage device of claim 11 wherein said method further comprises the step of appending indicators to said electronic document for delineating said identification envelope.</p>	<p>Claim 18 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent and U.S.P. 5,005,200.</p> <p>See Claim 8.</p>	<p>Claim 18 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent and U.S.P. 5,005,200.</p> <p>See Claim 8.</p>
<p>19. The program storage device of claim 11 wherein said identification envelope comprises information identifying materials used by said verifying party to verify the identity of said</p>	<p>Claim 19 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent.</p> <p>See Claim 9.</p>	<p>Claim 19 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent.</p> <p>See Claim 9.</p>

<p><b>U.S. Patent No. 5,872,848</b></p>	<p><b>Dziewit et al., U.S. Patent No. 5,031,214</b></p>	<p><b>Bisbee et al., U.S. Patent No. 5,748,738</b></p>
<p>originating party.</p>		
<p>20. The program storage device of claim 11 wherein said identification envelope is computer encoded.</p>	<p>Claim 20 is invalid as being obvious over Dziewit in view of the prior art admitted by the '848 patent. See Claim 10.</p>	<p>Claim 20 is invalid as being obvious over Bisbee in view of the prior art admitted by the '848 patent. See Claim 10.</p>