E-Commerce Update: Electronic Leases – Origination through Securitization

Panelists:
- Madelyn Law – Dell Financial Services
- Jack Stose – eOriginal, Inc.
- Margo Tank – Buckley Kolar LLP
- Berk Washburn – Key Equipment Finance

2004 Legal Forum
New Orleans, Louisiana
May 2-4, 2004
Agenda

- Electronic Chattel Paper: Overcoming Barriers to eLease Adoption
- Revised UCC 9-105 Requirements for Electronic Chattel Paper
- SPERS and AFSA eContracting Models
- eLease Operational Models: Vaulting and Registries
- Electronic Chattel Paper in the Automotive Finance Industry: eContracting and eSecuritization
  - DealerTrack: Industry Finance Aggregator
  - DaimlerChrysler: Captive Finance
  - Questions and Resources
Electronic Chattel Paper: Overcoming Barriers to eLease Adoption
“Companies Need An Electronic Equivalent - ‘A Parallel Solution Set’ - Of Processes From the Paper-Based World to Secure B2B Transactions”.

- Peter Miller
  J. P. Morgan Chase’s LabMorgan
  Computer World

“Our next challenge is the management, negotiation, storage, pooling, sale & securitization of e-contracts to capture the ultimate benefits of secondary market financing.”

- Mark O’Neil
  CEO of DealerTrack

Need for Electronic Chattel Paper

The Challenge

Need a process & system for creating electronic documents that are:

**Unique**: meaning there is only one authoritative copy

**Identifiable**: meaning an authoritative copy can be differentiated from all other documents

**Authentic**: meaning the creator of an authoritative copy is authorized & linked to the document.

**Unalterable**: meaning an authoritative copy can not be changed without detection.

**Transferable**: meaning ownership and custody of an authoritative copy can be legally transferred
Automating the various stages in the Financial Transaction Lifecycle

Application Integration Platform

Signature Capture
- Content/data capture
- Create documents
- Negotiation and underwriting
- Digital signatures
- Document packaging and transmission
- Regulatory filing or submissions

Management and Vaulting
- Execution
- Content and signature verification
- Document meta-data management
- Comprehensive auditing
- Servicing and view access

- Pooling/Rating
- Transfer of ownership
- Vault-to-Vault Transfers

Creation

Execution

Storage & Archival

Securitize

ELA Legal Forum 2004
Electronic Document Software and Functional Requirements

Securitization and Syndication
- Transaction Management and Document Aggregation
- Creation of Pools or Bundles of Transactions
- Electronic Transfer of Ownership of Transactions or Pools

Authoritative Copy
- Full compliance with UETA, E-Sign and Revised Article 9
- Views differentiated from Original Document
- Unique identifiable and unalterable
- Owner of the transaction/document determines all actions
- Authorization is required for copies or revisions

Document Repository
- Secure storage and version control
- Metadata Management
- Document History
- Roles & Access Rights
- Workflow/Transaction Processing

Electronic Signatures
- Guarantees Authenticity
- Document Integrity
- Non-repudiation
- Limited compliance with UETA & E-Sign

DM/eCM Solution
Registry/Vault
PKI Solution
Digital Signing
Revised UCC 9-105 Requirements for Electronic Chattel Paper
Article 9, 9-105

1. A single authoritative copy of the record or records exists which is unique, identifiable and, except as otherwise provided in numbered clauses 4, 5, and 6 below, unalterable;

2. The authoritative copy identifies the secured party as the assignee of the record or records;

3. The authoritative copy is communicated to and maintained by the secured party or its designated custodian;

4. Copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the participation of the secured party;

5. Each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

6. Any revision of the authoritative copy is readily identifiable as an authorized or unauthorized revision.
SPERS and AFSA

eContracting Models
SPeRS

Standards and Procedures for Electronic Records and Signatures
SPeRS Overview

- Founded by EFSC (Electronic Financial Services Council) and principals of Buckley Kolar LLP
- Broad multi-industry participation
- Guidelines, procedures, checklists and strategies for e-signature systems development
- High-level, technology-neutral advice
- Release 1.0 binder available now ($295)
- www.spers.org
SPeRS Release 1.0 Coverage

- Authentication
- ESIGN Consent / Agreement to Use Electronic Signatures and Records
- Agreements, Notices and Disclosures
- Signature
- Record Retention
American Financial Services Association

ANSI X9 Standards
eLease Operational Models

eVaulting and Registries

Mortgage (MERS) Example
eOriginal Vault Process

Transferable Authoritative Copies
Content Origination

“Create the document for execution”

• Documents created using existing workflow and document management systems.
• Electronic forms can be used to populate user-specific data into enterprise standard templates (e.g. LiquidOffice).
• Users continue to utilize familiar collaboration platforms (e.g. DealerTrack).
Apply Signature

“Customer applies signature to document”

- User presented with appropriate disclosures necessary to enable electronic contracting.
- Electronic (holographic) signatures are captured using an electronic signing pad (e.g. InterLinks, Topaz).
- Digital signatures may use hardware (e.g. SmartCard) or software based tokens
- Signature binding can be applied on the client machine or back at the server.
Verification & Validation Process

“Vault verifies privileges and signatures”

- eCore verifies a user’s ability (privilege) to submit the document to vault.
- Signed document package “opened” by the vault.
- eCore validates all signatures applied to the document (e.g. RSA, Identrus).
- eCore verifies the integrity of the document by application of its integrated PKI infrastructure.
“Vault applies time-stamped wrapper”

- eCore captures the date & time from a trusted time source.
- Date & time stamp sealed with the signed document using the dedicated eCore digital certificate.
- Sealed documents are stored within the vault, creating the authoritative copy.
- Return digital receipt to document submitter.
"Vault maintains secure access controls"

- Maintains transaction and document specific access controls.
- Maintains time-stamped and digitally signed logs of all selected events.
- Provides secure watermarked view of original documents.
- Enforces document retention and destruction rules.
Securitization / Syndication

“Selling to the secondary markets”

- Bundling of transferable records (e.g. installment contracts/leases/transactions) into pools.
- Securitization of pools into the secondary market.
- Syndication of pools into the secondary market.
- Ability for seller to automatically retain eCopies of transferred records.
- Provides Rating Agency approval / audit capability.
Mortgage eNote Registry Example

- Concept originated in eMortgage Workgroup
- MBA ResTech Committee took over, formed Task Force in 2002
- ResTech & Task Force released Requirements Document in Mar 03
- MBA Board passed resolution supporting single eNote Registry concept (and supporting MERS as logical choice for provider)
- MERS in production in April 2004!
The National Registry is…

- a centralized database that provides Section 16 Safe Harbor for electronic Notes (eNotes)
- intended to track and maintain information on eNotes that have been created using the industry standard MISMO SMART Document format
- the official record of who “controls” or owns the eNote and where it is vaulted
The National Registry will NOT...

- store eNotes or copies of eNotes
- track paper notes
- involve the transfer of funds (it is not a book entry system)
Requirements and Assumptions

- eNotes must contain language which references the National Registry to identify their Controller
- All parties interacting with the National Registry must have executed membership agreements with the National Registry
- Industry must standardize around a single National Registry
Vault and Registry Process Flow Example

Service Ordering:
- MI
- Credit
- Valuation
- Flood
- Hazard
- Title

*eNotes*

Source: Harry Gardner Presentation at NHEMA
eLeasing experience

IBM Credit – eOriginal ASP
GE Capital - eOriginal ASP
Dell Financial Services
Key Equipment Finance
What will the benefits be for the Leasing Industry?

- Competitive market advantage—reduced transaction cycle time leading to increased market share and profits
- Cost reduction—hard cost savings in management and delivery of paper document, transmission and vaulting expenses, “soft” savings from productivity gains due to fewer errors
- Improved customer service—enabling 24 x 7 customer self service for document-related questions and inquiries
- Reduced risk—control of document distribution and signature by remote lessees and third parties
- Minimal impact on existing origination process—relatively fast implementation time; easy integration into existing processes
- eSecuritization
Electronic Chattel Paper in the Automotive Finance Industry: eContracting and Securitization

- DealerTrack: Industry Finance Aggregator
Automotive Financing Industry

**DealerTrack’s Goal:** To become the leading on-line platform for end-to-end execution of retail installment contracts in automotive.

**System requirements:**
- Integrated secure vault
- Creation of “authoritative copy”
- Manage comprehensive ownership record
- Archival of “authoritative copy” for term plus seven years
- Pooling for securitization
- Support for supplementary documentation (i.e. application for title, invoices) in electronic or image form

- Platform available in 23,000 dealers and 70+ major auto lenders with 2.4 million credit applications per month
- eContracting in production with ...
Automotive eContracting Volume

**Vertical Market:** Financial institutions funding the sale and securitization of automotive retail installment contracts.

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of new/used autos sold annually in US</td>
<td>57 Million+</td>
</tr>
<tr>
<td>% Financed by banks &amp; captives</td>
<td>70%</td>
</tr>
<tr>
<td>Potential annual vehicle eContracting transaction volume</td>
<td>40 Million</td>
</tr>
</tbody>
</table>
Automotive eContracting

- Credit Applications (Credit Apps)
  - New Prime
  - New Sub-Prime & Leasing
  - Used Prime
  - Used Sub-Prime

Timeline
- 2003
- 2004
- 2005
- 2006

Sub-Segment Adoption

- eSecuritization
- eSignatures
Automotive Financing Industry

Company Information: DaimlerChrysler offers financial and other automotive services through DaimlerChrysler Services (DCS), including the DealerCONNECT online AutOrigination to 2000 dealers.

E-Signature Solution Goals:
- Extend AutOrigination to eContract and eSignature system
- Reduce contract errors and improve customer satisfaction
- Improve profitability for dealers and DCS and reduce charge-backs
- Improve processing efficiencies
- Reduction of paper contracts and other required forms
- Automate contract compliance
- Reduction of contract obsolescence and distribution costs
- Real-time reporting of Incentive Program performance

E-Securitization
Questions and Resources
e-Commerce Law Resource List

The following sites provide substantive information on legal issues that pertain to electronic documents and electronic signatures.

http://www.nccusl.org/
Website for the National Conference of Commissioners on Uniform State Laws (NCCUSL). Provides a searchable index of introductions and adoptions of current uniform and model acts with links to the summaries and final acts, new topics under discussion and drafting projects. Also with a link to the University of Pennsylvania below.

http://www.law.upenn.edu/library/ulc/ulc_frame.htm
The official site for the National Conference of Commissioners on Uniform State Laws (NCCUSL) located on the University of Pennsylvania School of Law website - provides information on the current status of uniform and model acts being drafted and/or the final versions of such acts. The Uniform Electronic Transactions Act (UETA) and the Revised UCC Article 9 – Secured Transactions – can be located on this site.
http://www.bakerinfo.com/ecommerce/
Website of the law offices of Baker & McKenzie’s ecommerce department (Chicago). It tracks the rapidly changing legal developments in ecommerce and is a valuable resource for current laws regarding ecommerce in state, federal and international arenas. Updated on a regular basis.


Excellent article outlining the basics of electronic signatures and the legal issues surrounding the authenticity and integrity of electronic documents.

http://www.perkinscoie.com/
Website of the law offices of Perkins Coie in Seattle. This is a valuable resource for current case law citations in a variety of practice areas – references U.S. court cases and international cases of especially high interest that address specific issues of Internet-related law, or that reach decisions that, although not directly related to the Internet, have significant implications for Internet legal issues.

http://www.abanet.org/buslaw/efss/
Website of the Subcommittee on Electronic Financial Services (SEFS), Business Law Section of the American Bar Association. This site provides links to follow new legal and policy developments in Electronic Financial Services. Click on Web Resources to find the on-line library which provides articles on a variety of financial service topics and electronic commerce case law citations/links.

http://www.cybersecuritieslaw.com/
Web site devoted to securities regulation and the Internet - Produces the CyberSecuritiesLaw Tribune, a regular update on developments in securities law and regulation with links to original source material.
SECTION 5
RECORD RETENTION

SPeRS Version 1.0 09

STANDARD 5-7. TRANSFERABLE RECORDS AND ELECTRONIC CHATTEL PAPER

SPeRS STANDARD 5-7

If the system is intended to manage the creation, execution, transfer and/or storage of electronic equivalents of negotiable promissory notes, bills of lading, warehouse receipts, retail installments sales contracts, debt obligations secured by personal property, or leases of tangible personal property, the System Design Team should consult with legal counsel or compliance personnel to determine the special requirements for:

- Controlling the transfer of ownership of the Electronic Record,
- Storing the Electronic Record, and
- Protecting the Electronic Record from unauthorized alteration.

PRINCIPLE

The new eCommerce laws recognize electronic equivalents to negotiable promissory notes, documents of title (bills of lading and warehouse receipt), and chattel paper (retail installment sales contracts, debt obligations secured by personal property, or leases of tangible personal property). However, in order to use the electronic equivalents of these documents, special care must be taken in designing and administering the Record management and retention systems.

CONSIDERATIONS

Discussion

As a general rule, the new eCommerce laws take a passive approach to amending existing law; they validate the use of Electronic Records and signatures, but do not create new types of Transactions or substantive rules for enforcing legal rights. For example, the rights and obligations of a purchaser of goods under Article 2 of the UCC remain the same whether the sales contract is in writing or is an Electronic Record. The eCommerce
laws permit an Electronic Record to serve as the sales Agreement, but do not invent a new type of sales contract or any new substantive rights in the seller or purchaser.

However, in order to create legal parity for electronic Transactions involving certain kinds of paper documents, a more proactive approach was required. Special rules have been created for the management and retention of electronic equivalents for:

- Negotiable paper promissory notes
- Chattel paper (e.g. retail installment sales contracts, promissory notes secured by an interest in personal property, and equipment leases), and
- Paper documents of title (i.e. warehouse receipts and bills of lading)

In broad terms, each of these types of paper documents evidences an obligation owed by the person issuing the paper document to another person named in the document. For example, a promissory note evidences an obligation to repay a debt. A warehouse receipt represents an obligation by the warehouse operator to deliver goods stored in the warehouse to the owner of the receipt.

The paper document is considered “negotiable” under commercial law if its terms and conditions meet specific criteria. Paper documents meeting these criteria “reify” the obligations they represent; that is, physical delivery of the paper document itself to the transferee, coupled with the transferor’s signed declaration of an intent to transfer (either written on the document or attached to it), constitute almost absolute proof of the transferee’s right to enforce the underlying obligation. This is because the physical transfer of the paper document provides the transferee, and others to whom the paper document is displayed, a high degree of confidence that the obligation is genuine and that the holder of the paper document is entitled to performance. The significance of negotiability is twofold; first, it creates an efficient mechanism for transferring performance rights to other Transaction Participants, and second, under the proper circumstances the transferee possessing such a paper document is granted a number of special rights under the law. Under appropriate circumstances these rights permit the transferee to:

- Enforce the negotiable document in spite of certain defenses the obligor may have against a prior transferor, and
- Avoid claims by third parties to own an interest in the negotiable document or a right to enforce the underlying obligation.

The special rights granted to the transferee of a negotiable paper document have significant commercial value. They simplify Transactions and lower costs. They also provide the owner with liquidity, since the obligations may be easily and quickly converted into cash by sale to a transferee, who can purchase the negotiable document confident of its enforceability against the obligor. When combined with the speed and efficiency of Transactions based on Electronic Records, these attributes of negotiable documents offer the potential for a variety of new, more efficient ways of doing business.
Accommodating the law of negotiability is one of the most significant challenges faced by any scheme to replace writings with Electronic Records. By definition, a unique Electronic Record cannot be physically transferred via telecommunication; any transmission of the Record results in a new Record at the receiving end, not the physical transfer of the original, with no certainty that the original has been destroyed. Transferring physical possession of the media storing an Electronic Record offers no help; first, resorting to physical transfer of the storage media undermines the principle reasons for using Electronic Records in the first place, ease of transferability, and second, since an Electronic Record can be copied repeatedly without any ability to distinguish the original from the copies, physically turning over a copy of the Record provides no guarantee that an indistinguishable copy has not been retained by the transferor. For these reasons, the assumptions underlying existing rules for negotiability do not work well in an electronic environment. Mere possession of a copy of an Electronic Record, with an electronic statement of transfer, does not provide the same level of confidence associated with paper-based documents.

In general, an Electronic Record can be used in place of one of these negotiable paper documents if:

- The Electronic Record contains only the same terms and conditions that are permitted in the written equivalent,
- The Electronic Record is signed,
- For negotiable promissory notes and documents of title, the issuer of the Electronic Record has expressly agreed that it will be treated as a “Transferable Record,”
- The method used to keep track of a transfer of interests in the Electronic Record reliably establishes the identity of the person entitled to “control” (meaning control the transfer of interests in) the Electronic Record.

A key question should be considered by the System Design Team for administering these types of Electronic Records is whether the method for registering a transfer of interests “reliably establishes” the identity of the person entitled to control the Record. A failure to meet this requirement may be fatal to a claim for status as the equivalent of a holder of a negotiable document. Note that failure to maintain control does not mean that the underlying obligation can’t be enforced against the obligor – it just means that the transferee may not get the special rights that a holder of the paper document would get with respect to defenses and/or third party claims.

The new eCommerce laws establish a set of rules to help determine whether the system design “reliably establishes” the identity of the person in control (the “Safe Harbor”). Use of the Safe Harbor is mandatory for electronic chattel paper, but optional for electronic equivalents of negotiable promissory notes and documents of title. To qualify

1 This requirement doesn’t apply to electronic chattel paper, except for an electronic equivalent of a negotiable promissory note that becomes part of a chattel paper package.

©EFSC 2004
for control under the Safe Harbor, the Transferable Record must be created, stored, and assigned in such a manner that:

- Once the Record is signed, there is always a single authoritative copy of the Record that can be identified and distinguished from all other copies of the Record;
- After being signed, the authoritative copy cannot be altered without the alteration being detected and identified as either an authorized or unauthorized change;
- The authoritative copy in some way provides a way to identify the person in “control” of the Record;
- The authoritative copy is transmitted to and maintained by either the person in control or someone acting as a custodian for that person; and
- Control can only be transferred with the approval of the person already in control.

In addition to establishing control, there is sometimes a business reason to preserve the option of converting the Electronic Record into a paper original. This is a particularly difficult process, since it necessarily entails both de-certifying the authoritative copy of the Electronic Record and creating, presumably via printout, a paper original that includes the obligor’s signature – this means that the obligor’s permission to convert to paper and intent to create a “wet ink” signature via printout needs to be captured at the time the Electronic Record is signed.

Checklist

(a) The System Design Team should consult with the business managers and legal counsel or compliance personnel to determine:

(i) Whether the Electronic Records to be managed and retained by the system will include any of the following:

(A) An electronic equivalent to a negotiable promissory note,
(B) An electronic equivalent to a document of title, or
(C) Electronic chattel paper.

(ii) Whether it is necessary or desirable for the system to be designed to provide the special features necessary to preserve “control” of the Electronic Record so that transferees of the Electronic Records

---

2 There is existing precedent for doing this. Original letters of credit are often created by having a letter of credit print on a teletype machine at a financial institution – the printout is stamped “original” and becomes the original signed letter of credit.
receive the same rights as transferees of equivalent paper documents.

(iii) Whether it will be necessary or desirable to establish a procedure for converting the Electronic Record into a paper original.

(b) If control is to be established, then the System Design Team must:

(i) If the Records are an electronic equivalent to a negotiable promissory note or document of title, determine whether:

(A) To implement the Safe Harbor, or

(B) To implement another process or procedure to establish control.

(ii) If the Records are electronic chattel paper, implement the Safe Harbor.

(c) In implementing the Safe Harbor, the System Design Team must:

(i) Implement a method to distinguish the authoritative copy of the Record from other copies. Strategies the System Design Team may wish to consider include:

(A) Storing the Electronic Record within a secure system that will not permit the creation of other copies (other than backup copies for restoration of the secure system).

(B) Storing the Electronic Record within a secure system that will not permit the creation of other copies (other than backup copies for restoration of the secure system) without in some manner distinguishing them from the authoritative copy. Methods for distinguishing the non-authoritative copies may include:

(1) Embedding a legend or watermark in the copy stating that it is a non-authoritative copy, or

(2) Assigning a specific identifier to the authoritative copy.

(C) Establishing a secure registry for tracking the authoritative copy that (i) is referenced in the Electronic Record itself and (ii) permits the current control party to provide information to the registry on the authoritative copy’s current location. The location of the authoritative copy may be:
(1) Fixed permanently at the time of creation,

(2) Established by consulting a person identified in the registry as able to advise on the specific location of the authoritative copy, or

(3) Capable of being moved from one location to another over time, with the new locations being reported to the registry and the registry updated to reflect the current location.

(ii) Implement a method for preventing undetected alterations of the Record after signing. Strategies the System Design Team may wish to consider include:

(A) Using a signature process that protects the Electronic Record from undetected alteration;

(B) Using a cryptographic process applied by the system or a trusted third party to protect the Electronic Record from undetected alteration;

(C) Using an audit log to track and Record all changes and alterations made to the authoritative copy of the Record;

(D) Isolating the authoritative copy on a secure system that does not permit access to the completed Record for purposes of alteration.

(iii) Implement a method for establishing control over the authoritative copy, including identification of the control party, storage of the authoritative copy by the control party or a designated custodian, and control over authorizing transfer.

3 The level of specificity of the provided location information may vary – it may be a listing of the specific location, a general location, or point to the document custodian for additional information.

4 Note that as a general matter, protection against alteration becomes relevant at the time the first signature is associated with the Electronic Record. After the first signature, it is usually true that the only alterations that are authorized without further consultation and authorization by the signers are the association of additional signatures.

5 Note that there is nothing in the eCommerce laws that would prevent the use of a nominee as the named control party, just as a nominee could be the holder of a paper negotiable document.
(A) Strategies the System Design Team may wish to consider include:

(1) Requiring the current control party, or a designated agent, to authorize a transfer of control of the authoritative copy to a new control party within a single secure system storing the authoritative copy.

(2) Requiring the current control party, or a designated agent, to authorize any transmission of the authoritative copy from the current secure system to a different secure system that will be storing the authoritative copy for a new control party.

(3) Establishing a secure registry for tracking control of the authoritative copy that (i) provides information on the current control party and the location of the authoritative copy, (ii) is referenced in the Electronic Record itself, and (iii) requires authorization from the current control party, or a designated agent, for the registry to reflect a transfer of control.

(B) The System Design Team may wish to consider:

(1) Whether any transfer authorized by the current control party must be confirmed by the proposed new control party, or an authorized agent, before the transfer is considered effective.

(2) Whether the current control party, or its designated custodian, must agree in advance to automatically serve as a temporary designated custodian for the new control party in the event there is some difficulty in transferring or transmitting the authoritative copy to the new control party or its designated custodian.

(3) If a registry is being used to track the location of the authoritative copy, whether either automated or manual confirmation of the post-transfer location of the authoritative copy as reflected in the registry must be obtained.

(C) In general, control should be established and maintained from the time the authoritative copy is fully executed and has been submitted or delivered to the original obligee for effect. If a registry is being used to monitor control and the
Record will not be registered immediately upon execution and delivery, the System Design Team should consider including in the Record a statement that the original obligee may only transfer the Record after registering it on the identified registry.

(iv) The System Design Team may wish to consider providing a method for converting the Electronic Record into a paper original. The System Design Team should consult with legal or compliance personnel to determine whether any specific requirements for converting the Record have been established by regulators or potential purchasers of the Record, such as a secondary market or other institutional investor. In addition, the System Design Team should consider:

(A) In such cases, when the Electronic Record is converted to paper, designing the document management system to reflect that an authoritative copy of the Electronic Record no longer exists.

(B) Including in the Electronic Record language indicating the obligor’s assent to be bound by the Record regardless of whether it remains in electronic form or is reduced to paper, and expressing the obligor’s intention that he or she will be bound by the obligor’s signature regardless of the medium.

(C) Branding the paper copy with a statement that it is the written original of a Record previously held in electronic form, and including or associating with the paper copy the complete ownership chain from the original payee through the current control party, with each transfer expressed in traditional language of negotiable indorsement, either with or without recourse, as appropriate. The System Design Team may wish to consider:

(1) In systems that Record transfers in the electronic chattel paper itself using transfer certificates, referencing transfers by incorporating appropriate indorsement language into the certificates, which print out as part of the paper document, or

(2) In systems that use an ownership registry, by having the system act as the electronic agent for each transferor, supplying the indorsement chain based on information contained in the ownership registry, with the indorsements printing out as part of the
tangible promissory note or chattel paper, or on an allonge accompanying any such instrument.

(3) In either case, including with the indorsement either a holographic or other manuscript or typed signature for each endorser.

(4) Establishing system rules or a transfer procedure that reflects the endorser’s intent to adopt the signature when it is printed out as part of the transformed Record.

(D) Providing that only one copy of the authoritative copy may be printed out with a “written original” brand or designation. Once that copy is printed, the system for holding the Transferable Record in electronic form may automatically reflect that the authoritative copy has been “papered out” to the party in control at the time the Record was converted to paper form, and that any electronic copy of the Record displayed or referenced by the system is no longer the authoritative copy.

COMMENTARY

The UETA and ESIGN refer to the electronic equivalents to negotiable promissory notes and documents of title as “Transferable Records.” Revised Article 9 uses the phrase “electronic chattel paper” for electronic equivalents to traditional chattel paper. In general, the New eCommerce Laws grant the transferee of an interest in an Electronic Record the same special rights as the holder in due course of a negotiable promissory note, or the purchaser in good faith of a negotiable document of title or traditional chattel paper, if:

- The Electronic Record contains only the same terms and conditions that are permitted in the written equivalent,
- The Electronic Record is signed,
- For negotiable promissory notes and documents of title, the issuer of the Electronic Record has expressly agreed that it will be treated as a “Transferable Record,”

Legally, the Agreement to treat the Electronic Record as a Transferable Record may either be placed in the Transferable Record itself, or in a separate Record. As a practical matter, however, placing the Agreement in a separate Record will create complications in transferring the rights – for example, how will the transferee know that the transferred Record has been issued subject to the required Agreement?

This requirement doesn’t apply to electronic chattel paper, except for an electronic equivalent of a negotiable promissory note that becomes part of a chattel paper package.
• The method used to keep track of a transfer of interests in the Electronic Record reliably establishes the identity of the person entitled to “control” (meaning control the transfer of interests in) the Electronic Record.

A key question, in designing a system for administering these types of Electronic Records, is whether the method for registering a transfer of interests “reliably establishes” the identity of the person entitled to control the Record. A failure to meet this requirement may be fatal to a claim for status as the equivalent of a holder or purchaser of a negotiable document. Note that failure to maintain control does not mean that the underlying obligation can’t be enforced against the obligor – it just means that the transferee may not get the special rights that a holder or purchaser of the paper document would get with respect to defenses and/or third party claims.

The Safe Harbor

As discussed above, use of the Safe Harbor is mandatory for electronic chattel paper, but optional for electronic equivalents of negotiable promissory notes and documents of title. To qualify for control under the Safe Harbor, the Electronic Record must be created, stored, and assigned in such a manner that:

• Once the Record is signed, there is always a single authoritative copy of the Record that can be identified and distinguished from all other copies of the Record;
• After being signed, the authoritative copy must be unalterable without the alteration being detected and identified as either an authorized or unauthorized change;

8 UETA § 16(a) and (b); ESIGN §201(a)(1) and (b). There is a subtle limitation on the handling of Transferable Records contained in this definition. The UETA and ESIGN permit parties to convert writings to Electronic Records, with the electronic copy serving as an evidentiary equivalent to the writing, which may be destroyed. See UETA §§ 12, 13; ESIGN §101(d)(3). This is not the case with a Transferable Record, where the issuer of the Electronic Record must expressly consent to application of the Transferable Record provision to the Record. The obligor on a pre-existing paper promissory note has not agreed to be the issuer of an Electronic Record. Therefore, even if the obligor agreed in writing to waive the terms of UCC §3-604 (providing that intentional destruction of a promissory note constitutes release of the debt), scanning and shredding the promissory note would not satisfy the requirements of the UETA or ESIGN.

9 In addition, ESIGN (but not the UETA) requires that an electronic equivalent to a negotiable promissory note be secured by an interest in real property. ESIGN §201(a)(1)(C).

10 Official Comment 3 to UETA § 16; Revised Article 9 §9-105.

11 The term “unalterable” should not be taken too literally. Practically speaking, no Record is unalterable. Ordinary writings may be altered, and so may almost any type of Electronic Record. All Records are also subject over time to decay and deterioration. The requirement that a Transferable Record be unalterable is modified by UETA § 16(c)(6), which permits revisions that are readily identified as authorized or unauthorized. In other words, the UETA does not require that a
• The authoritative copy in some way provides a way to identify the person in “control” of the Record;
• The authoritative copy is transmitted to and maintained by either the person in control or someone acting as a custodian for that person; and
• Control can only be transferred with the approval of the person already in control.12

The first requirement of the Safe Harbor, for an “authoritative copy,” reflects a reality of the electronic environment – there is no such thing as an “original” document that can be transferred from person to person. The transmittal of an electronic document results in the creation of a new copy, not the physical transposition of the existing copy. A copy, to qualify as the authoritative copy, must meet three criteria – it must be unique, identifiable, and (except as otherwise provided) unalterable.

“Unique” is not otherwise defined, and it therefore should be understood in its simple dictionary sense, that is, the authoritative copy must have a characteristic that distinguishes it from other copies. That characteristic may be provided by technology, or by process or Agreement. For example, an authoritative copy stored within a controlled-access system may be provided with a unique control number, or be held in a specified server or other location that makes it distinguishable from other copies.

As a practical matter, if a Record is unique, then almost by definition it is identifiable, so that the second criterion for an authoritative copy appears redundant. The most sensible interpretation of the “identifiability” rule is that the document management system being used, or the Agreement of the Transaction Participants, must explicitly define the authoritative copy in terms of its unique characteristic. In other words, an Agreement or system rule presumably must specify or describe the unique feature that identifies the authoritative copy, and how that unique feature can be accessed or confirmed.

Finally, the third criterion for an authoritative copy is that the Record must be unalterable; but this general rule is subject to three significant exceptions. First, the Record may be altered to reflect a new, authorized assignee of the Record. Second, the Record may be altered to reflect whether or not it is the authoritative copy. And finally, the Record may be altered so long as the authoritative copy reflects whether the revision is authorized or unauthorized. Essentially, the authoritative copy must be unalterable without detection, but may be altered so long as the changes can be tracked and it can be determined whether or not the change was authorized.

The authoritative copy does not have to be static over time. The copy that qualifies as the “authoritative copy” at one time, during or after the Transaction, need not be the same copy that qualifies as the authoritative copy at another time. All that is required is that, at

Transferable Record be unalterable in a metaphysical sense, but only that it be unalterable without detection.

12 UETA §16(c); ESIGN §201(c).
any given moment, there be a single authoritative copy. So, for example, the authoritative copy may be transmitted from one location to another, which technically requires the reproduction of the authoritative copy at the place of receipt and destruction or de-certification of the authoritative copy at the sending location. The UETA and ESIGN expressly contemplate that the authoritative copy may be transferred by telecommunication.\footnote{UETA §16(c)(3); ESIGN §201(c)(3).}

The authoritative copy must, in some way, be tied to a method for identifying the current party in control. This may be done by having evidence of the transfer of control integrated into the authoritative copy itself, or by having the authoritative copy logically associated with a methodology for tracking control, so that a person viewing the authoritative copy also is alerted, and has access, to the evidence of control.

The other feature of the Safe Harbor that merits closer examination is the requirement that all non-authoritative copies of the Electronic Record be readily identifiable as such. Once again, the new eCommerce Laws do not specify a technological or process solution to this requirement. For example, the requirement could presumably be met by storing the authoritative copy in a closed system that automatically “brands” all non-authoritative copies as such. As an alternative, the Record itself could give notice of the location at which the authoritative copy is stored, so that by definition all copies stored at other locations are not the authoritative copy. As yet a third example, the Record itself could provide for reference to system rules or a registry for determination of the location of the authoritative copy, so that anyone having access to the Record is on notice that they must check the system rules or registry to identify the authoritative copy.

One of the most significant questions about the Safe Harbor is the appropriate practical method for:

- Evidencing a transfer of control, and
- Identifying the authoritative copy of the Transferable Record.

**TWO MODELS FOR SATISFYING THE SAFE HARBOR**

As various industries have begun addressing this question, two principal conceptual models have emerged for handling these issues:

- A “single document management system” model in which all Transaction Participants, from the originator to the final investor, have access to the authoritative copy on a single system. Ownership and control are related to access rights, and change dynamically as ownership of the Electronic Record is transferred.\footnote{It should be noted that at this time there appears to be little interest in a “multiple document management system” model without the use of a central registry to handle control issues and to}

---

\footnote{UETA §16(c)(3); ESIGN §201(c)(3).}

©EFSC 2004
A registry model, in which the authoritative copy itself may be transmitted from system to system and from one physical location to another, but a central registry referenced in the Electronic Record itself keeps track of the current owner and the location of the authoritative copy.

Each model addresses these four functions:

- Identifying the authoritative copy of the Electronic Record
- Establishing the location of the authoritative copy
- Identifying the party in control of the Electronic Record
- Effecting a transfer of control of the Electronic Record

The E-Vault Model

The first model is one that takes advantage of a self-contained, secure environment and leverages the fact that with an Electronic Record it is control over access, and not physical location, that is of chief importance to the owner of the Record. In this model, an authoritative copy is created and stored in a secure electronic environment (“E-Vault”). Every party requiring access, from the originator or broker creating the documentation and obtaining signatures, to the ultimate investor/owner, obtains access via the E-Vault. Access may be direct, or through a portal. In this model, the authoritative copy of the Electronic Record is stored in the E-Vault.

The E-Vault employs a secure methodology to keep track of the identity of the control party for each Electronic Record. Each purchaser of the Electronic Record will take control by becoming the identified party in control within the secure E-Vault environment. The operator of the E-Vault would be required to enter into an “Electronic Storage Agreement” with each owner/purchaser establishing certain system rules and defining operational reliability and security standards. The Electronic Storage Agreement would also establish that the E-Vault operator has no interest in the authoritative copies or the underlying data, and would extend certain protections to the owner of the Electronic Record in the event that the operator was experiencing financial or operational difficulties.

The E-Vault model should be in compliance with the Safe Harbor so long as:

- The system complies with properly designed system rules and appropriate functional and operational controls to insure system and Record integrity.
The methodology used for establishing control is effective and requires the consent of the current control party, or its authorized agent, for a transfer of control to occur.

The person operating the system is either the party in control of the Electronic Record or a designated custodian of that party.

The fully executed authoritative copy is protected within the E-Vault from undetected alterations, and an audit log is maintained of the authority for each alteration that occurs.

Each copy of the authoritative copy, whether in electronic or printed form, is in some way marked (e.g. with a watermark or legend) to indicate that it is not the authoritative copy.

The Registry Model

For markets in which many originators sell to multiple purchasers in an open secondary market, and there is a constant movement of servicing rights from one entity to another, the single system model has limitations. The mortgage industry, for example, relies heavily on negotiable promissory notes and on the fungibility of mortgage loans. The notes evidencing the mortgage debt are sold to multiple investors. The investor is sometimes selected several weeks or months after the loan is closed. For this reason a single document management system may not be appropriate. This is particularly true in the residential mortgage business where the number of Transactions that must be accommodated and the number of entities participating in each Transaction in one capacity or another can be very large. As a result, a registry for tracking transfers of control and the location of the authoritative copy might be considered preferable.

In this model, control over the right to transfer ownership of an Electronic Record, and the right to designate the location of its authoritative copy, are to be determined solely by reference to a registry. The primary preconditions for the registry are:

- All Transaction Participants interested in creating and transferring control in the Electronic Record would agree to look to the centralized registry to track control.
- Each Electronic Record would:
  - Contain language placing anyone viewing it on notice that its true controller must be determined by reference to the central registry, and
  - State that all copies that are not at the location referenced in the registry are non-authoritative.
• The registry would (a) identify the controller, and (b) reference the location of the Transferable Record’s current authoritative copy.\textsuperscript{15,16}

• A transfer of control would be accomplished by receipt of a secure authorization to transfer from the transferor, and, in at least one model, a secure authorization of transfer from the transferee.

• The custodian of the authoritative copy would be either the current owner of the Transferable Record or the current owner’s designated custodian.

• The Transferable Record would be held in such a manner that the controller or the controller’s custodian is able to distinguish the authoritative copy from other copies.

The unique characteristic of the authoritative copy of the Transferable Record is established within the controlled system storing the Record. The authoritative copy is held by the controlling party or its authorized custodian, and is logically associated with a registry entry of the identity of the control party and the location of the authoritative copy. The registry is referenced in the Electronic Record itself.\textsuperscript{17} Control may only be transferred with the consent of the current controlling party, and the authoritative copy may not be altered, once executed, without detection.

The use of a registry system for identifying the custodian of a Transferable Record was expressly contemplated by the drafters of the UETA.\textsuperscript{18} Because the Transferable Record itself points to the registry, a party looking at any copy of the Transferable Record would be on inquiry notice as to the identity of the control party. The use of the registry to identify the location of the authoritative copy should work in much the same way – a party looking at any copy of the Transferable Record is on notice that the location of the authoritative copy is established in the registry. If the copy they are viewing is not the copy identified in the registry, then it is not the authoritative copy. In this way, every copy of the authoritative copy should be regarded as “readily identifiable.”

Note that the registry may be run by any trusted Participant, including a Participant in the registry that has interests represented in the registry. Because the registry is a reference database, and not a custodian, there is no legal reason to require that the operator of the registry be an independent Participant.

\textsuperscript{15} These elements are drawn from a presentation given by John A. Richards, Associate General Counsel of Fannie Mae, at the American Bar Association’s 2002 Annual Meeting.

\textsuperscript{16} Note that the “location spotting” function of the registry could be accomplished in one of two ways – either by specifying the location in the registry, or by providing information on the identity of the custodian holding the authoritative copy and directing the inquiring party to the custodian for further information on the authoritative copy’s precise location.

\textsuperscript{17} The use of such an arrangement to satisfy the requirements of UETA §16(c) is discussed in Official Comment 3 to Section 16.

\textsuperscript{18} See Comment 3 to UETA §16.
The inclusion in the Transferable Record of an Agreement recognizing that the registry designates the authoritative copy should not violate the requirement that the Transferable Record contain only those terms and conditions permissible for a negotiable promissory note under Article 3 of the Uniform Commercial Code. UCC §3-104(a)(3) provides that a negotiable instrument may not contain an undertaking or instruction by the payee to do any act in addition to the payment of money. The Agreement concerning the location of the authoritative copy does not require the payee to take any action, and furthers the purposes of UETA §16 and ESIGN §201. The inclusion in the Transferable Record of supplemental Agreements furthering the purpose of the statute was expressly contemplated by the UETA’s drafters.

“Branding” of non-authoritative copies would not be necessary in a system where the location of the authoritative copy is established within a secure registry. In effect, the ability to distinguish the authoritative copy from all other copies arises not from the branding of all other copies as non-authoritative, but as a result of all Transaction Participants being on notice, via the registry, that all copies not stored at the designated location are non-authoritative. For this reason, it should be possible to transfer the authoritative copy from one custodial server to another as an adjunct to such a registry system. By Agreement, the authoritative copy is the copy designated in the registry as such. If the Transferable Record refers parties to the registry for the location of the authoritative copy, and if the registry is updated by the current owner to designate the new location, then the copy at that new location becomes the authoritative copy by definition.

19 UETA §16(a)(1); ESIGN §201(a)(1)(A).
20 See Official Comment 2 to UETA §16 (Transferable Record itself may include Agreement to treat Record as Transferable Record).
New eCommerce laws make possible the widespread replacement of paper documents with electronic records. They also enable the broad use of electronic signatures. Many businesses have begun converting their operations to avail themselves of the enormous advantages offered by electronic records systems.

While the new eCommerce laws permit the use of electronic records and signatures, they also require that electronic systems and processes meet specific standards for:

- Obtaining consent to use electronic records and signatures,
- Presentation of information,
- Execution of signatures and creation of agreements,
- Record retention,
- Printing, and
- Delivery.

Failure to meet those standards may impair the enforceability of electronic records. As a result, companies are being forced to invest significant time, effort and manpower in answering questions about how to handle the practical, routine aspects of electronic transactions. Much of this time and effort could be avoided if industry-wide standards for these elements of electronic transactions could be established.

To address this problem, industry leaders have undertaken a cross-industry initiative to establish commonly understood “rules of the road” available to all parties seeking to take advantage of the powers conferred by ESIGN and UETA. The product of this initiative is the Standards and Procedures for Electronic Records and Signatures (“SPeRS”).

WHAT IS SPeRS?

SPeRS is:

- A set of guidelines, procedures, checklists and strategies for developing systems to create, deliver, sign, manage and transfer legally enforceable electronic records and signatures in commercial and consumer transactions. Intended to help companies develop cross-discipline system design teams for implementing electronic commerce.
- Focused on the behavioral aspects of the interaction between participants in the transaction. SPeRS is technology neutral.

SPeRS will:

- Permit businesses to establish a common understanding with internal team members and vendors concerning the methodology for designing eCommerce systems,
- Assist in establishing industry standards for commercially reasonable, enforceable structures and processes, and
- Help provide the customer with a “common experience” across various online transactions.

WHAT KINDS OF ISSUES DOES SPeRS ADDRESS?

SPeRS’ 30 Standards, and the supporting checklists, address dozens of issues related to the use of electronic records and signatures. Examples include:

- Describing the risks and liabilities associated with using a PIN or password.
- Obtaining a consumer’s consent to use electronic records and signatures.
- Selecting a signature process that is appropriate for the transaction.
- Establishing the intent to sign an electronic record.
- Effectively delivering information in an electronic environment.
- Using hyperlinks and other devices used in referencing, displaying, and drawing attention to information and disclosures.
- Strategies for effective record retention.

See the attached Table of Contents for more information.
WHO PARTICIPATED IN CREATING SPeRS?

**Drafting Committee Members**

Adobe Systems Incorporated  
American International Group, Inc.  
Charles Schwab & Co., Inc.  
CitiMortgage, Inc.  
Dell Financial Services L.P.  
Fannie Mae  
First American Title Insurance Company  
Freddie Mac  
General Electric Mortgage Insurance Corporation  
Harland Financial Solutions  
Harris Investor Services LLC  
Intuit Inc.  
Massachusetts Mutual Life Insurance Company / MassMutual Financial Group  
Mortgage Guaranty Insurance Corporation  
PricewaterhouseCoopers  
Principal Financial Group  
Swiss Re Life & Health America, Inc.  
TIAA-CREF  
VeriSign, Inc.  
Wells Fargo Home Mortgage  
Zions Bancorporation / Identrus, LLC

**Advisors**

ACORD  
Alliance of American Insurers  
American Bankers Association  
American Council of Life Insurers  
American Financial Services Association  
National Association for Variable Annuities  
Mortgage Bankers Association of America  
National Multi Housing Council  
Securities Industry Association  
Software & Information Industry Association

**Observers**

beTRUSTed  
Esurance Inc.  
NewRiver, Inc.  
Republic Mortgage Insurance Co.  
RPost  
RouteOne LLC  
Safedocs  
Silaenis Technology  
SwiftView, Inc.  
Wave Systems Corp.

**Reporters/Counsel for SPeRS**

R. David Whitaker, Wells Fargo Home Mortgage, Inc.  
Jeremiah S. Buckley, Buckley Kolar, LLP  
Margo H. K. Tank, Buckley Kolar, LLP

**HOW DO I ORDER SPeRS?**

SPeRS Version 1.0 is available now for $295.00 per hardbound copy, plus $15.00 shipping and handling per copy. To order online visit [www.spers.org](http://www.spers.org). To order via telephone, contact Laura Kenney at Buckley Kolar, LLP at (202) 349-8068.
SPeRS Table of Contents

How to Use SPeRS

Overview of UETA and ESIGN

Glossary

Section 1 – AUTHENTICATION AND AUTHORITY
  Standard 1-1: Identifying and Evaluating the Appropriate Authentication Strategy – Creating the Relationship
  Standard 1-2: Identifying and Evaluating the Appropriate Authentication Strategy – Credentials
  Standard 1-3: Providing Consumers Information Concerning the Distribution of Risk for Unauthorized Transactions
  Standard 1-4: Establishing the Authority of Representatives

Section 2 – CONSENT TO USE ELECTRONIC RECORDS AND SIGNATURES
  Standard 2-1: General Agreement to Use Electronic Records and Signatures
  Standard 2-2: Applicability of the ESIGN Consumer Consent Process
  Standard 2-3: The ESIGN Consumer Consent Disclosures
  Standard 2-4: The ESIGN Consumer Consent Disclosures - Format And Timing
  Standard 2-5: Obtaining the Consumer's Affirmative Consent – Methods and Timing
  Standard 2-6: Reasonable Demonstration of Access

Section 3 – AGREEMENTS, NOTICES AND DISCLOSURES
  Standard 3-1: General Principles for Display and Presentation of Information
  Standard 3-2: Delivering and Displaying Records and Information
  Standard 3-3: Delivering And Displaying Records And Information -- Retention Of Records By Other Transaction Participants
  Standard 3-4: Indicating Agreement
  Standard 3-5: Acknowledging Access or Delivery
  Standard 3-6: Conspicuous Disclosure
  Standard 3-7: Using Hyperlinks and Other Navigational Cues

Section 4 – ELECTRONIC SIGNATURES
  Standard 4-1: Selecting a Signature Process
  Standard 4-2: Providing Information On The Signing Process
  Standard 4-3: Establishing the Intent to Sign
  Standard 4-4: Associating a Signature with a Record
  Standard 4-5: Attributing a Signature
  Standard 4-6: Electronic Agents

Section 5 – RECORD RETENTION
  Standard 5-1: Meeting Accuracy, Accessibility and Retention Requirements
  Standard 5-2: Verifying the Integrity and Accuracy of Electronic Records/The Physical and Logical Environment
  Standard 5-3: Verifying The Consistency and Integrity of Electronic Records
  Standard 5-4: Document Conversion
  Standard 5-5: Vendor Relationships
  Standard 5-6: Interaction with Governmental Agencies
  Standard 5-7: Transferable Records and Electronic Chattel Paper

Appendix A – SUMMARY OF SPeRS STANDARDS

Appendix B – SUMMARY OF SPeRS PRINCIPLES