Framework for

Control over Electronic Chattel Paper

Compliance with UCC §9-105

From the Working Group on Transferability of Electronic Financial Assets, a Joint Working Group of the Committee on Cyberspace Law and the Committee on the Uniform Commercial Code of the American Bar Association Business Law Section and The Open Group Security Forum

Prepared by:
Mattias Hallendorff (ABA Working Group on Transferability of Electronic Financial Assets)
and Mike Jerbic (The Open Group)

ABA
Defending Liberty
Pursuing Justice

ABA Section of
BUSINESS LAW
Practical Resources for the Business Lawyer

in association with

THE *Open* GROUP
Making standards work®

The views expressed in this Guide are not necessarily those of any particular member of The Open Group or the American Bar Association.

The views expressed herein have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the policy of the American Bar Association.

Framework for Control over Electronic Chattel Paper

ISBN: G061

Document No.: 1-931624-60-7

Published by The Open Group and the American Bar Association, January 2006.

Any comments relating to the material contained in this document may be submitted to:

ogpubs@opengroup.org

or:

copyright@abanet.org

contents

Preface

Control over electronic chattel paper is a collaborative project between the Working Group on Transferability of Electronic Financial Assets – a joint working group of the Committee on Cyberspace Law and the Committee on the Uniform Commercial Code of the American Bar Association Business Law Section – and The Open Group.

This Guide is intended to provide a framework for analyzing when and if a party is able to show "control" over electronic chattel paper (ECP) pursuant to UCC §9-105.[1]

We believe that the need to show control over ECP is likely to arise in two situations. First, transactional participants and users of a "Control System" will need to be convinced that the legal requirements are met in order for various transactions to proceed. A Control System will need to work within a "Control Environment" that provides a sound basis for trust in the integrity of the Control System. A Control Environment must also have certain features in order for the Control System to meet the requirements for control under UCC §9-105. Developers of Control Systems and Control Environments must be able to show and explain how and why their systems satisfy the requirements of UCC §9-105.

Second, the ultimate test of whether a Control System and a Control Environment working together actually provide control under UCC §9-105 will be in the context of a legal proceeding challenging a secured party's claim of perfection by control. The secured party must be able to demonstrate how and why the Control System meets the requirements of UCC §9-105.

This Guide frames the issue of control under UCC §9-105 in a question and answer format based on a technology-neutral control model. We

[1] The Official Text and Comments of the Uniform Commercial Code (UCC) is published by and copyright of the American Law Institute and the National Conference of Commissioners on Uniform State Laws. It is available in hardcopy from Thompson/West, Uniform Commercial Code, 2005 Ed. The American Law Institute, National Conference of Commissioners on Uniform State Laws, Official Text and Comments, 2005. An authorized online version of the UCC, without the comments, is available from the legal Information Institute at Cornell Law School at www.law.cornell.edu/ucc/ucc.table.html.

believe that system developers, with the help of legal counsel, will need to be able to answer the questions set forth below, both in order to provide a marketable product/service and to enable the users of their products/services to obtain predictable legal results.

About The American Bar Association and the ABA Section of Business Law

The American Bar Association (ABA) is the largest voluntary professional association in the world. With more than 400,000 members, the ABA provides law school accreditation, continuing legal education, information about the law, programs to assist lawyers and judges in their work, and initiatives to improve the legal system for the public. The Mission of the American Bar Association is to be the national representative of the legal profession, serving the public and the profession by promoting justice, professional excellence, and respect for the law. Further information is available at www.abanet.org.

The ABA Section of Business Law serves the public, the profession, and its nearly 60,000 members by furthering the development and improvement of business law, educating Section members in business law and related professional responsibilities, and helping Section members serve their clients competently, efficiently, and professionally. The Section, through its committees, often provides comment on policy to Congress and government agencies. It supports a robust offering of CLE in all aspects of business law and publishes a library offering over 100 titles in addition to The Business Lawyer, the nation's premier journal of business law. The Section is devoted to promoting full and equal participation in Section activities and in the practice of business law by minorities, women, and persons with disabilities. Further information is available at www.ababusinesslaw.org.

About The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry's premier certification service.

Further information on The Open Group is available at www.opengroup.org.

The Open Group has over 15 years' experience in developing and operating certification programs and has extensive experience developing and facilitating industry adoption of test suites used to validate conformance to an open standard or specification.

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical and Product Standards and Guides, but which also includes White Papers, Technical Studies, and Business Titles.

A catalog is available at www.opengroup.org/bookstore.

Trademarks

Acknowledgements

The authors gratefully acknowledge the contributions of the many people who gave freely of their time and wisdom to improve this document, including in particular the following:

Bob Blakley of IBM Corporation
Ian Dobson of The Open Group
Jane Kaufman Winn of University of Washington School of Law
Richard Keck of Duane Morris LLP
Nick Mansfield of Royal Dutch Shell
Steve Mathews of Articsoft Corporation
Richard Newman of Mayer Brown Rowe & Maw LLP
Linda Rusch of Hamline University
Paul Shupack of Benjamin N. Cardozo School of Law
Ron Williams of IBM Corporation

Chapter 1

Introduction

In the world of tangible chattel paper, multiple pieces of paper could make up the chattel paper (such as a note and a separate security agreement). There are often multiple copies of the same item of chattel paper. One of those items is typically marked “original” and the other copies marked “copy”. While filing an effective financing statement in the appropriate place may perfect a security interest in chattel paper under UCC §9-310, a possessor of tangible chattel paper can obtain superior rights in the chattel paper under UCC §9-330. To obtain those superior rights, the possessor must possess the copy of the tangible chattel paper marked “original”.

With this paper world in mind, the drafters of Revised Article 9 developed the concept of “control” for electronic chattel paper (ECP) – UCC §9-105. The drafters intended that the elements of control as stated in UCC §9-105 be the electronic analog of possession of the copy of tangible chattel paper marked “original”. Thus the idea of “record or records” recognized that multiple writings could make up one “item” of chattel paper. The UCC §9-105 designation of a “single authoritative copy” of ECP that was “unique and identifiable” was intended to be the functional equivalent to the “original” copy of tangible chattel paper. What makes the tangible copy of an item of chattel paper “single”, “authoritative”, “unique”, and “identifiable” is the ability to mark it as the “original”. For ECP, the assumption was that technological systems would be developed that would permit an electronic copy to be tagged as the “original”, thus making it distinguishable from other non-authoritative copies.

The drafters of Revised Article 9 also recognized that in the world of tangible chattel paper, assignments of and revisions to that chattel paper could be noted on the tangible “original”. Similar provisions for noting authorized revisions and assignments of ECP were provided for in the UCC §9-105 definition of control.

Finally, unlike the securities arena where regulated intermediaries provide record keeping ability for determining rights and obligations with respect to intangibles such as un-certificated securities and security entitlements, the drafters of Revised Article 9 had to consider who would maintain the electronic records that comprise ECP. UCC §9-105 requires that either the secured party or its designated custodian maintain the electronic records comprising an item of chattel paper. Although the trustworthiness and integrity of the system for maintaining the ECP records are critical to the control concept, Revised Article 9 does not dictate how the trustworthiness or integrity of such a system should be demonstrated.

In comparison to tangible chattel paper, ECP by its very nature may be perceived as having an increased risk of error or other problems. This is due to the ease with which large amounts of data can be stored, moved, or lost in an electronic environment as well as the sheer amount of data stored electronically as compared to that stored in tangible form. In addition, electronic systems are able to make perfect, identical copies of electronic information. This alone makes compliance with UCC §9-105 challenging. Such compliance will require a combination of people, processes, and technology.

It is important to note that a Control System and its Control Environment need not protect against all possible exploitations of the Control System. As noted in the Official Comments to UCC §9-105, the standards for determining whether a secured party has control of ECP should not be more stringent than those applicable to determining possession of the original copy of tangible chattel paper. However, a Control System and Control Environment must address the unique and inherent risks associated with maintaining and transferring large quantities of electronic data with limited physical resources.

The Official Comments to UCC §9-105 state that "achieving control under [UCC §9-105] requires more than the agreement of the interested parties that the elements of control are satisfied". The Official Comments also point out that "control of [ECP] would not be defeated by the possibility that the secured party's interest *could* be subverted by the wrongful conduct of a person (such as a custodian) acting on its behalf". Determining whether the elements of control are satisfied requires a factual analysis of the Control System and Control Environment to determine whether the two, working together, create a sufficient degree of confidence in their integrity and capacity to perform the functions for which they were designed. However, the requirements are not so stringent as to demand from Control Systems and Control Environments absolute perfection. UCC §9-105 allows for the frailties of both human and machine processes and systems.

UCC §9-105 provides as follows:

"A secured party has control of electronic chattel paper if the record or records comprising the chattel paper are created, stored, and assigned in such a manner that:

1. *A single authoritative copy of the record or records exists which is unique, identifiable, and, except as otherwise provided in paragraphs (4), (5), and (6), 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."*

Chapter 2

Control Analysis

UCC §9-105 substitutes the concept of "control" of the electronic records making up ECP for "possession" of tangible chattel paper. To understand and analyze the concept of control, as used in the UCC, it is helpful to first consider the linguistic definition of the term "control". Merriam-Webster's dictionary definition of control includes:

Verb: "to exercise restraining or directing influence over"

Noun: "power or authority to guide or manage"

Control systems engineering relies on a well developed, technology-neutral, theoretical base to model, develop, and implement systems that deliver predictable, assured results from a range of valid requests, or inputs. Together with UCC §9-105, this control analysis uses a classical model of closed loop control systems engineering and applies it to the objective of a secured party exercising restraining or directing influence over ECP.

No system of any complexity is absolutely free of defects or vulnerabilities. If a Control System is assumed to have some degree of undiscovered defects or vulnerabilities, the question becomes one of degree of reliability and confidence. Because a Control System cannot detect its own defects or vulnerabilities, there must be a means for detecting them that is outside the Control System. We refer to this set of people, processes, and technology as a "Control Environment". A Control System's Control Environment addresses the question of the degree of confidence one can have in the integrity of the Control System. A Control Environment consists of such things as the process and control of system design, the process and control over system operations, the trustworthiness of the people using and operating the system, the business processes outside of the technology of its related Control System, and security technology that adds trust to the input to the Control System. A failure in any of these areas compromises the trustworthiness of a Control System. A Control Environment also provides the mechanisms by which unauthorized actions or the occurrence of unauthorized events within its related Control System may be detected.

A Control System and its Control Environment are made up of:

1. The people managing and using the system

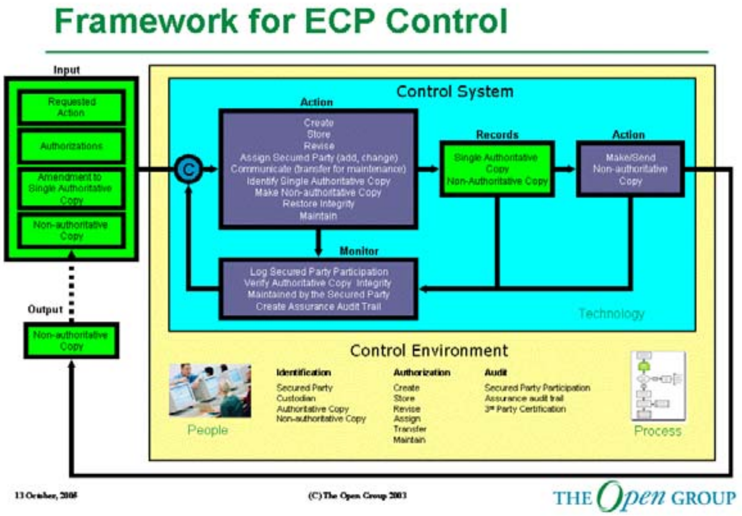
2. The technological and human processes for managing and using the system
3. The technology used to run the system

Each of these needs to be analyzed in assessing whether a Control System together with its Control Environment meets the requirements of UCC §9-105 for control of ECP. The questions set forth below are intended to relate to all three parts of the system. The responses to the questions are intentionally somewhat generic. Specific answers will depend on the specific characteristics of a particular Control System and Control Environment. Specific answers may address some or all of:

1. The people managing and using the system
2. The technological and human processes implemented for purposes of managing and using the system
3. The technology used to run the system

Depending on the design of a Control System and Control Environment, the importance of the three parts of the system may vary and the emphasis put on each part will vary accordingly.

The following flow chart sets forth the functions required of a Control System with a Control Environment. It does so from a system perspective and will facilitate a technology-neutral assessment of whether a total system meets the legal requirements established in UCC §9-105.



Framework for ECP Control

Input

Requested Action

Authorizations

Amendment to Single Authoritative Copy

Non-authoritative Copy

Output

Non-authoritative Copy

Control System

C

Action

Create
Store
Revise
Assign Secured Party (add, change)
Communicate (transfer for maintenance)
Identify Single Authoritative Copy
Make Non-authoritative Copy
Restore Integrity
Maintain

Records

Single Authoritative Copy
Non-Authoritative Copy

Action

Make/Send Non-authoritative Copy

Monitor

Log Secured Party Participation
Verify Authoritative Copy Integrity
Maintained by the Secured Party
Create Assurance Audit Trail

Technology

Control Environment

People

Identification
Secured Party
Custodian
Authoritative Copy
Non-authoritative Copy

Authorization
Create
Store
Revise
Assign
Transfer
Maintain

Audit
Secured Party Participation
Assurance audit trail
3rd Party Certification

Process

13 October, 2005

(C) The Open Group 2003

THE Open GROUP

Notes on the Framework for ECP Control

1. The framework for control consists of a Control System operating within the larger context of a Control Environment.
2. A Control Environment establishes the people and processes within which the technology can operate to a predictable assurance level. A Control Environment can also monitor its related Control System for failures that the closed loop Control System cannot self-detect. An analogous example is an intrusion detection system. While the intruder has penetrated a Control System undetected, an intrusion detection system – outside the Control System but within the Control Environment – detects the intrusion, allowing recovery outside the normal operation of the primary Control System. Through its external controls, the Control Environment provides additional assurance that the Control System is working as expected.
3. A Control System has three operational components:
   a. The action component which executes requests defined by inputs of a non-authoritative copy of ECP, amendments to existing ECP, and authorization information legitimizing the request
   b. The monitor which logs and analyzes the outcome of those actions
   c. The comparator function which assesses differences between what was requested and what actually occurred

   By responding to and recovering from differences between what was requested and what actually occurred, the closed-loop Control System provides for predictable results within a limited range of error conditions or system flaws. This predictability is what establishes the difference between a command process and control process.
4. Control System outputs are non-authoritative copies of ECP. Single authoritative copies of ECP must remain inside the Control System; hence they cannot be Control System outputs.

A trap for the unwary is to rely on a “command process” rather than a “control process”. The former, which is commonly used both in technology processes and human management processes, assumes that commands, once given, are carried out. Execution of a command may lead to the intended consequences, but the execution of the command alone does not create control. A control process incorporates the additional steps of verifying that commands have been carried out and providing for specific responses if such verification fails.

The following chapter provides questions that need to be answered by anyone assessing whether a Control System and its Control Environment satisfy the requirements for “control” set forth in UCC §9-105 as well as the answers that generally will need to be provided to those questions. The answers are intended to be technology-neutral. For each Control System and Control Environment, the actual answers will be different depending on each system’s specific design. Substantively, however, those answers need to address the statements made in the form of answers set forth below.

Chapter 3

Questions & Answers

3.1 Control System

3.1.1 Input

Question 1	**Who are the parties that may provide input into the Control System (“Authorized Participants”)?**
Answer	Secured party, designated custodian (if any), and new/added secured parties only.
Commentary	Authorized Participants are those persons that may interact with a Control System in such a way as to modify ECP maintained on the Control System. While it is correct to consider a debtor’s relationship to the secured party and an item of ECP, a debtor does not provide any input into a Control System. Only a secured party and its designated custodian may provide input into a Control System. The debtor has no impact on whether control exists under UCC §9-105. Related to this question is the issue of what input may be provided into a Control System by each Authorized Participant. Although this issue may have significant legal and practical implications, it is not relevant for purposes of establishing control under UCC §9-105.
Question 2	**By what means are inputs made?**
Answer	By such means as may allow for: 1. The verification and authentication of the Authorized Participant 2. The subsequent verification and authentication of the input
Commentary	In this context, “verification” means determining that all required elements of the input are present for a particular action, including the presence and authority of the Authorized Participant. Verification establishes that a Control System is able to maintain the integrity of the input. Verification does not require either that the input content is accurate or that the Authorized Participant has legal (as opposed to system access) authority. In short, the fact that a Control System allows for “junk in, junk out” is not relevant to whether

	there is “control” under UCC §9-105.
Question 3	**What inputs may be made into a Control System?**
Answer	1. Requested actions 2. Authorizations 3. Amendments to ECP 4. Non-authoritative copy of ECP
Commentary	Electronic records can be of a wide variety, such as scanned copies of existing hard copies, certificates and time stamps, etc. UCC §9-105 does not address the content of electronic records or whether they satisfy the legal requirements for enforceability of chattel paper.

3.1.2 Actions

Question 4	**How is an Authorized Participant identified and associated with each action?**
Answer	In a manner that allows, with respect to each applicable action, the verification, authentication, and its association to the Authorized Participant.
Commentary	The actions that may be taken by an Authorized Participant are to: 1. Create ECP 2. Store and maintain ECP 3. Revise ECP 4. Assign ECP 5. Communicate ECP 6. Identify the single authoritative copy of ECP 7. Make a non-authoritative copy of ECP Once the Authorized Participant is authenticated, the Control System and the Control Environment need to be able to associate the Authorized Participant with each action taken within the Control System. Note that maintenance of ECP includes the creation of back-ups and the restoration from back-ups. Also, identification of the single authoritative copy of an item of ECP need not require an affirmative action of

	identification. The identification of the single authoritative copy as such follows from its attributes and existence within a Control System. The designated custodian may (and probably must, as a practical matter) take certain actions in relation to the single authoritative copy of ECP. However, the actions of the designated custodian should be limited so as not to have legal ramifications beyond establishing "control".
Question 5	**How is the secured party's participation ensured in connection with making copies of or revisions to ECP that add or change an identified assignee?**
Answer	The secured party's participation is verified and authenticated either through the secured party's direct participation, or through a verified and authenticated delegation to a designated custodian.
Commentary	UCC §9-105 (4) is the only provision requiring the participation of a particular party. This provision does not preclude a secured party from delegating its participation to its designated custodian. Also note that, except for UCC §9-105 (4), UCC does not require that only Authorized Participants take the necessary actions. However, as a practical matter as well as to meet other legal requirements, a Control System should be designed so that only an Authorized Participant is allowed to take Authorized Actions and that only the secured party can take certain Authorized Actions.
Question 6	**How are non-authoritative copies of a single authoritative copy of ECP readily identifiable as such?**
Answer	Actions within a Control System are monitored and logged so as to allow verification and authentication of the single authoritative copy and revisions thereto.
Commentary	The mechanisms for verifying the single authoritative copy of an item of ECP will identify any non-authoritative copies. All copies other than the authoritative copy of ECP are, by definition, non-authoritative copies. In particular, all copies of an item of ECP that exist outside of a Control System are non-

	authoritative copies. A Control Environment provides for monitoring and logging actions within the Control System.

3.1.3 Output

Question 7	**What are the outputs for a Control System?**
Answer	Only non-authoritative copies.
Commentary	The single authoritative copy of ECP can only exist within a Control System. Accordingly, any copy (whether in tangible or electronic form) existing outside of the Control System is a non-authoritative copy. A non-authoritative copy may, however, be a certified copy.

3.1.4 Monitoring

Question 8	**How are the actions taken within a Control System, the single authoritative copy of ECP, and any non-authoritative copies within the Control System monitored?**
Answer	1. Authorized Participant participation is logged. 2. Single authoritative aopy integrity is verified. 3. Maintenance and storage of ECP by the secured party (or its designated custodian) is verified. 4. An audit/log trail of actions taken is maintained.
Commentary	Monitoring any system requires two components: (1) a log of Control System activities, and (2) an analysis of those activities that demonstrates that the system performed functions as requested. The log should contain a record of at least five dimensions of system activities: (1) who requested/performed an action; (2) what action did the requestor authorize; (3) when (date and time) did the request occur and when did it get fulfilled; (4) how was the requested action implemented; and (5) what functions did the system perform to implement the requested action? In addition to these primary

	dimensions, secondary dimensions such as where did the request occur and why was it made may be important to establish context and provide additional evidence in support of the legitimacy of an activity. Using the log as a data source, people, processes, and technology *inside and outside* of a Control Environment can analyse the log to determine whether the Control System is performing as expected. These logging and analysis capabilities also serve to verify the integrity of ECP maintained within a Control System.

3.1.5 Verification

Question 9	**How are monitoring processes used to verify actions taken or not taken?**
Answer	Real-time/periodical verification processes are used to compare the results of requested actions to the requests. Monitoring processes serve as the data foundation for verification.
Commentary	A Control System can examine its logs and other monitoring information to determine whether requested actions have been completed and what, if any, remedial action must be taken. Within a certain range, a Control System can detect and recover from its own faults. Outside of a Control System, but within its Control Environment, people, processes, and technology can separately evaluate the Control System logs and other monitoring information to determine whether the Control System is performing as expected. This analysis permits discovery of intrusions, unauthorized system configuration changes, system vulnerability explanations, and faults from which the Control System is unable to recover on its own. All Control System processes (action, comparator, and monitor) must be verifiable outside of the Control System but within the Control Environment. Since the Control Environment so heavily relies upon the monitor process for Control System verification, the monitor should have additional controls or integrity

	checks built in to establish the trustworthiness of this foundational information.

3.1.6 Single authoritative copy/New Input

Question 10	**How are non-authoritative copies of ECP communicated and revised?**
Answer	In a manner that provides for distinguishing a non-authoritative copy from the single authoritative copy.
Commentary	Non-authoritative copies may be important – they may, for example, serve as inputs into a Control System used to create a single Authoritative copy of an item of ECP. Communication and revision of non-authoritative copies may be important to the operation of the overall Control System, and a Control System may protect them accordingly to ensure their trustworthiness. A Control System must have one or more of the following: (1) a means to identify and control the single authoritative copy within the Control System (any copy of ECP outside of the Control System, whether in tangible or electronic form, is a non-authoritative copy) and (2) a means to identify all non-authoritative copies of ECP within the Control System. Note that UCC §9-105 does not require a Control System to create non-authoritative copies. Some system designs may only use single authoritative copies of an item of ECP, making unnecessary any capability to distinguish, communicate, or revise non-authoritative copies.

3.2 Control Environment

In order for a Control System to provide control over ECP, there must be sufficient confidence in the Control System's integrity. Its Control Environment must be designed to establish the basis for this confidence.

3.2.1 Identification

Question 1	**What identification and authentication mechanisms and processes are used to identify and authenticate:** **1. A secured party** **2. A designated custodian** **3. The single authoritative copy of an item of ECP?**
Answer	Means, features, and processes that comply with appropriate financial industry identification and authentication standards (based on industry and type of transaction).
Commentary	One means of establishing the identity of the single authoritative copy of ECP is by its location, since the single authoritative copy can only exist within a Control System. Any copy existing outside of the Control System is, by default, a non-authoritative copy.

3.2.2 Authorization

Question 2	**What authorization mechanisms and processes are used to authorize the following actions with respect to ECP:** **1. Creation** **2. Storage and maintenance** **3. Revision** **4. Assignment** **5. Transfer** **6. Creation of non-authoritative copies of ECP?**

Answer	Means, features, and processes that comply with appropriate financial industry authorization standards (based on industry and type of transaction).
Commentary	Authorizations are based on legal, contractual, or business policy considerations; they are not derived from technical mechanisms. Once authorizations have been established, technical systems can implement them. UCC §9-105 authorizes only the secured party or its designated custodian to create, store and maintain, revise, assign, and transfer ECP. A Control Environment must reflect this requirement by providing the necessary foundation for reliable exercise of authority in technical systems. The authorization will rely upon authentication of the applicable Authorized Participant and audit trails demonstrating actions taken by the Authorized Participant. The ultimate objective of a Control Environment is to reduce the likelihood that an Authorized Participant can repudiate its actions or assert that an Authorized Action was requested but not carried out by the Control System.

3.2.3 Audit/Auditability

Question 3	**What overall audit processes are used and available to audit:** **1. Control System functions and features** **2. Required party participation** **3. Monitoring audit/log trail?**
Answer	Internal and third-party audit processes that provide for transparent and credible audit reports and certification.
Commentary	A Control Environment must collect, maintain, and analyse evidence to determine whether its Control System is performing in accordance with specification necessary to meet the requirements of UCC §9-105. Thus, a Control Environment's audit function is to verify the trustworthiness of its Control System. The main objectives of the analysis are to demonstrate

	that: (1) the Control System as initially deployed meets all of the specifications necessary to meet the requirements of UCC §9-105; (2) all system changes after initial deployment are authorized by the Authorized Participants; and (3) all information changes after initial deployment are authorized by the Authorized Participants. A Control System cannot declare itself trustworthy. Only through an analysis of the Control System's behaviour, system and functional logs, and other information outside of the Control System can its Control Environment determine that the Control System is trustworthy to the requisite degree. Determining the appropriate degree of trustworthiness in the absence of applicable industry standards would involve a risk assessment, including an assessment of the vulnerability of the Control System, the likelihood that any such vulnerability is exploited, and the value at risk in case the vulnerability is exploited.

3.3 Control System and Control Environment in Combination

Question 1	**How are non-authoritative copies of a single authoritative copy of ECP readily identifiable as such?**
Answer	Actions within a Control System are monitored and logged to allow verification and authentication of the single authoritative copy of ECP and the revisions thereto.
Commentary	Verifying and authenticating the single authoritative copy of ECP identifies all other copies as non-authoritative copies since all copies other than the single authoritative copy of ECP are non-authoritative. In particular, all copies of ECP that exist outside of a Control System are non-authoritative copies. A Control System's Control Environment provides for monitoring and logging actions within the Control System.

Question 2	**Can there be a certified copy of the single authoritative copy of ECP?**
Answer	Yes.
Commentary	Processes implemented by the Control System can certify that a non-authoritative copy is an exact duplicate of the single authoritative copy. If the non-authoritative copy is in tangible form, processes and people can certify that the tangible form is an accurate representation of the ECP. The ability to create certified copies of the single authoritative copy is not a requirement for achieving control under UCC § 9-105, but is important as a practical matter in order to be able to offer evidence of the content of the single authoritative copy.
Question 3	**How are non-authoritative revisions of a single authoritative copy of ECP readily identifiable as such?**
Answer	Actions within a Control System are monitored and logged to allow verification and authentication of the single authoritative copy of ECP and the revisions thereto.
Commentary	Verifying and authenticating the single authoritative copy of ECP maintains its integrity. A Control System together with its Control Environment must provide for both monitoring and auditability to permit periodic verification and authentication of the single authoritative copy of ECP. From the technical perspective, a Control System is likely to be designed so that it is unable to execute any unauthorized action. However, from a legal perspective, a Control System and its Control Environment must be able to track actions in such a manner that technically authorized actions but legally unauthorized actions can be distinguished. How this will be achieved will depend on the design of the Control System and its Control Environment, and encompass all three parts of the system: (1) the people managing and using the system; (2) the technological and human processes

	implemented for purposes of managing and using the system; and (3) the technology used to run the system.

3.4 Statutory Analysis

The statute contemplates that there can be more than one copy of the record or records comprising an item of ECP. However, there can only be a single authoritative copy of the records comprising the ECP. A “copy” of the record or records making up the ECP derives its authoritativeness from being:

1. Unique

2. Identifiable

3. Unalterable (except as specifically provided for in the statute)

The provisions of UCC §9-105 (1), as modified by subsection (4), (5), and (6), are the most challenging provisions to address in determining whether there is control over ECP. However, ECP must also be created, stored, and assigned in such a manner that the single authoritative copy:

1. Identifies the secured party as the assignee of the record or records

2. Is communicated to and maintained by the secured party or its designatedcustodian

3.4.1 Unique

The concepts of uniqueness and identification are closely related. The fact that a copy is identifiable as the single authoritative copy makes that copy unique. However, other data associated with an item of ECP (such as time and date of creation or modification of the records, and location of and method of storage) can more conclusively establish its uniqueness.

Question 1	**Is the record or records making up the ECP unique?**
Answer	Yes

Question 2	**What makes the ECP unique?**
Answer	Its designation within a Control System as unique by the Authorized Participant maintaining the ECP (the secured party or its designated custodian).
Commentary	Although an item of ECP is unique if it is so designated by the Control System in which it is maintained, uniqueness also requires sufficient confidence in the integrity of the Control System.
Question 3	**How is the ECP unique?**
Answer	Its existence within a Control System and the features of the Control System providing for uniqueness.
Commentary	The ECP derives its uniqueness from its designation as unique by the custodian of the ECP, its existence within a Control System, and the features and functions of the Control System that make the ECP unique, in reliance on the integrity of the Control System. Uniqueness can be derived from various data and information associated with the ECP based on both processes and technology.

3.4.2 Identifiable

In addition to being unique, the records that comprise the single authoritative copy of an item of ECP also must be identifiable as being the single authoritative copy of the particular ECP.

Question 4	**Are the record or records making up the ECP identifiable as the single authoritative copy of the record or records making up the ECP?**
Answer	Yes
Question 5	**What makes a record or records identifiable as the single authoritative copy?**
Answer	Their identification, within a Control System and by the custodian of the ECP (the secured party or its designated custodian), as the records making up the single authoritative copy of ECP.

Commentary	Identification of records as being the single authoritative copy requires reliance on and confidence in the integrity of the Control System in which the ECP is maintained.
Question 6	**How are the record or records making up the ECP identifiable as the single authoritative copy of the record or records making up the ECP?**
Answer	Its existence within a Control System and the features of the Control System providing for identification of the record or records making up the ECP as the single authoritative copy.
Commentary	The identification of record or records as the single authoritative copy of ECP is based on its existence within a Control System and the features of the Control System identifying a copy of ECP as the single authoritative copy, together with confidence in the integrity of the Control System. Identification of the records can be derived from various data and information associated with the ECP based on both processes and technology. The term “record” as used in Article 9 is intended to convey a technology-neutral approach to, among other things, memorializing terms of an agreement. The term also needs to be consistently interpreted in regards to both electronic and tangible chattel paper. An electronic record should not be subject to any more stringent requirements than a tangible record. Some have suggested that to satisfy the “single authoritative copy” requirement, the binary code that makes up the electronic record itself must be unalterable, unique, and identifiable. That suggestion should be rejected. In the tangible paper world, that would be tantamount to requiring that the molecules making up the paper and ink dots must be unique, identifiable, and unalterable.

3.4.3 Unalterable

The third requirement of UCC §9-105 to establish control over ECP is that, with certain exceptions, it is "unalterable". UCC §9-105 permits ECP to be alterable so long as:

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

2. Each copy of the single authoritative copy and any copy of a copy is readily identifiable as a copy that is not the single authoritative copy.

3. Any revision of the single authoritative copy is readily identifiable as an authorized or unauthorized revision.

In order to show that the records are alterable only within those exceptions, a Control System must address the following questions.

Question 7	**Is the single authoritative copy unalterable?**
Answer	No, probably not in absolute terms.
Question 8	**If not unalterable, how are revisions made?**
Answer	Within the Control System and subject to the protocols and procedures developed for making such revisions.
Commentary	Revisions are tracked within a Control System based on features and procedures of the Control System and its Control Environment that provides for verification of the integrity of the Control System.
Question 9	**How are revisions authorized?**
Answer	Through the ECP's existence within a Control System and the features of the Control System that provide for appropriate authorization to revise the ECP.
Commentary	Revisions are authorized within a Control System based on features and procedures of the Control System and its Control Environment that provides for verification of the integrity of the Control System.

Question 10	**Are revisions tracked and recorded?**
Answer	Yes
Question 11	**How are revisions tracked and recorded?**
Answer	Through the ECP’s existence within the Control System and its Control Environment and the features of the Control System providing for tracking of revisions.
Commentary	From the perspective of a Control System, actions taken by it will seem authorized; otherwise, the Control System would not take the requested action. Any discovery of unauthorized actions will occur outside of the Control System but within its Control Environment. Some Control Systems and associated Control Environments may be designed such that any revision is treated as unauthorized and only the creation of a new single authoritative copy of ECP replacing the existing single authoritative copy of ECP is acceptable. However, so long as there is confidence in a Control System’s integrity, as substantiated by its Control Environment, the Control Environment may be structured so as to allow for tracking of authorized and unauthorized revisions.
Question 12	**Are unauthorized revisions distinguishable and identifiable from authorized revisions?**
Answer	Yes
Question 13	**How are unauthorized revisions distinguishable and identifiable from authorized revisions?**
Answer	The ECP’s existence within the Control System and its Control Environment and the features of the Control System and its Control Environment provide for tracking and analysis of revisions.
Commentary	Although a Control System will make only Authorized Revisions to an item of ECP, it may be unable to distinguish a legally authorized action from a legally unauthorized action. Legally unauthorized revisions can occur through exploitation of a Control System’s vulnerabilities and defects, misuse of the Control System by Authorized Participants, or through

	compromised processes outside of the Control System. Because the Control System does not detect legally unauthorized revision, any unauthorized revision must be detected through mechanisms and processes contained in its Control Environment. The Control Environment, including the people, processes, and technology outside of its Control System, detects unauthorized revisions.
Question 14	**Is the secured party a required participant in connection with a transfer of the ECP from one assignee to another?**
Answer	Yes
Question 15	**How is the secured party a required participant in connection with a transfer of the ECP from one assignee to another?**
Answer	Through the features and functions of the Control System and its Control Environment requiring the secured party's participation.
Commentary	Assignments of ECP and related revisions thereto are authorized within a Control System based on features and procedures of the Control System and its Control Environment that verify the integrity of the Control System and the single authoritative copy of ECP before and after assignment.
Question 16	**Is a copy of the single authoritative copy of the record or records making up the ECP readily distinguishable from the single authoritative copy?**
Answer	Yes
Question 17	**How is a copy of the single authoritative copy of the record or records making up the ECP distinguishable from the single authoritative copy?**
Answer	Within a Control System, the features and functions of the Control System distinguish the single authoritative copy from any non-authoritative copies, and outside of the Control System, all copies are non-authoritative.
Commentary	The features and procedures of a Control System must be able to distinguish non-authoritative copies of ECP,

	and the record or records making up the non-authoritative copies of ECP, from the single authoritative copy of ECP, and the record or records making up the single authoritative copy of ECP, that exists within the Control System. ECP's existence within the Control System, and its Control Environment that maintains confidence in the integrity of the Control System, provides confidence in the integrity of the single authoritative copy of ECP.

3.5 Assignment and Transfer

In addition to the functional/system requirements set forth above, UCC §9-105 contains two additional technical requirements. The single authoritative copy of ECP must include information identifying any assignee of the ECP. Further, the single authoritative copy must be "communicated" to and "maintained" by the secured party (or its designated custodian). The assignment and transfer of an item of ECP does not destroy the ECP's character as the single authoritative copy.

Question 18	**Does the single authoritative copy of ECP identify the secured party as the assignee of the record or records?**
Answer	Yes
Question 19	**How does the single authoritative copy of the ECP identify the secured party as the assignee of the record or records?**
Answer	Through the features and functions of the Control System in which the ECP is maintained.
Commentary	Assignments of ECP and related revisions thereto are authorized within a Control System based on features and procedures of the Control System and its Control Environment that verify the integrity of the Control System and the single authoritative copy of ECP before and after assignment.
Question 20	**How are assignments tracked so that the single authoritative copy of ECP identifies the secured**

	party as the assignee of the record or records?
Answer	The features and procedures of the Control System in which the ECP is maintained identify the secured party as the assignee of the ECP from time to time.
Commentary	Assignments of ECP and related revisions thereto are authorized within a Control System based on features and procedures of the Control System. Assignment of the ECP within a Control System and its Control Environment maintains confidence in the integrity of the single authoritative copy of ECP before and after assignment.
Question 21	**Is the single authoritative copy of ECP communicated to and maintained by the secured party or its designated custodian?**
Answer	Yes
Question 22	**How is the single authoritative copy of ECP communicated to and maintained by the secured party or its designated custodian?**
Answer	The single authoritative copy of ECP is communicated within the Control System in which the ECP is maintained.
Commentary	Communication of the ECP is authorized and occurs within a Control System based on features and procedures of the Control System. A Control System's Control Environment verifies the integrity of the Control System and the single authoritative copy of ECP before and after communication. A single authoritative copy of ECP may also be communicated to a different Control System, provided, however, that any such communication must in such case be completed seamlessly from one Control System to another. The single authoritative copy of ECP can only exist within a Control System and must pass from the transferor Control System to the transferee Control System without existing outside of a Control System. In order to maintain control in connection with transfers from one Control System to another, the

	respective Control Environments are likely to be overlapping each other in scope.
Question 23	**How does the single authoritative copy of ECP retain its status as the single authoritative copy following communication to the secured party or its designated custodian?**
Answer	The communications occurs within the Control System in which the ECP is maintained.
Commentary	So long as the communication takes place within a Control System, the features and processes of the Control System together with its existence within its Control Environment provide for confidence in the integrity of the Control System and the single authoritative copy of ECP following communication to the secured party or its designated custodian. If a single authoritative copy of ECP is communicated to a different Control System, any such communication must be completed seamlessly from one Control System to another. The single authoritative copy of ECP can only exist within a Control System and must pass from the transferor Control System to the transferee Control System without existing outside of a Control System. In order to maintain control in connection with transfers from one Control System to another, the respective Control Environments are likely to be overlapping each other in scope.

About the Authors

Mattias Hallendorff

Mattias is an attorney with Dorsey & Whitney LLP in Minneapolis, Minnesota, practicing in the areas of domestic and international financial and commercial matters, including commercial loans, mergers and acquisitions, project financing, and banking and privacy regulations.

He is the co-chair of the ABA Joint Working Group on Transferability of Electronic Financial Assets. He lives in St. Louis Park, Minnesota with his wife and two daughters and can be reached at hallendorff.mattias@dorsey.com.

Mike Jerbic, CISSP, PMP

Mike is an independent consultant who specializes in high technology engineering and project management. With over 20 years' experience in hardware and software product development, engineering management, and IT project management, Mike's interest area is in solving complex, multifaceted problems that require a varied background and experience to solve, such as the control of electronic chattel paper.

Mike chairs The Open Group Security Forum and is a member of the American Bar Association's Business Law Section and many other technical professional associations. He holds bachelors and masters degrees in Electrical Engineering, with emphasis on controls and systems, from the University of California at Berkeley.

Mike lives in Cupertino, California with his wife and daughter. He can be contacted at smjerbic@trustedsystemsconsulting.com.