Massachusetts Legal Hackers
Blockchain Digital Signature

July 12, 2017 Mock Trial Initial Read Through & Discussion

The following Memo was contributed by Allyson N Hammerstedt, a new Massachusetts Legal Hackers member who we thank for both her written contributions and her active, constructive participation in the Mock Trial run through!

TO: MIT Legal Hackers/Dazza Greenwood
FROM: Allyson N. Hammerstedt
DATE: July 12, 2017
RE: Blockchain Digital Signatures Mock Trial – overview of procedural standards re foundation and evidentiary objections

How to Lay Proper Foundation for Witness

In order to satisfy that the electronic signature is authentic, Federal Rule of Evidence 901 identifies several factors:

> "This standard can generally be satisfied by evidence that (1) the computer equipment is accepted in the field as standard and competent and was in good working order, (2) qualified computer operators were employed, (3) proper procedures were followed in connection with the input and output of information, (4) a reliable software program was utilized, (5) the equipment was programmed and operated correctly, and (6) the exhibit is properly identified as the output in question."

State v. Swinton, 847 A.2d 921, 942 (2004). Extrinsic evidence regarding the authenticity of the digital signature as a condition precedent of admissibility is not required to establish that the "electronic message to which the digital signature is affixed has not been altered from its original form" and that the "digital signature corresponds to a specific public key pair." 31 C.F.R. § 370.39.

The person testifying about the electronic signature can use direct or circumstantial evidence to show the account that the digital signature was sent from, sufficient detail to

confirm that the party in question was the party who signed the document, and evidence that the party receiving the digital signature took action based on it.[1]

Likely Angles for Objection—Evidentiary Issues

Even after authenticating the electronic signature, there are other evidentiary issues for objecting.

The biggest evidentiary issue relates to hearsay. In Massachusetts, Mass. Gen. L. ch. 233, sec. 78 creates the business records exception. In order to satisfy the requirements for a business record, the document must be: "(1) made in good faith (2) in the regular course of business and (3) before the beginning of the civil or criminal proceeding where (4) it was the regular course of such business to make such memorandum or record at the time of such act, transaction, occurrence or event or within a reasonable time thereafter." Mass. Gen. L. ch. 233, sec. 78.

Relevance and prejudice are also arguments for objecting, but based on the facts of the mock trial, these arguments would not hold up because the document is at the center of the question about whether a breach occurred; therefore, it can be argued that the document is inherently relevant.

Other Notes From July 12 Massachusetts Legal Hackers:

- **See Comments:** Several questions, ideas and other comments contributed throughout this meeting appear as “comments” inserted at the relevant sections of this Google Doc (look to side panel on right).
- **See: Vectors of Attack** section below for potential grounds for objections & defenses
- **See: Next Steps** from July 12 Meeting immediately below Witness Examination script

Witness Examination

The following script is intended as a starting point to guide the process of entering Blockchain-Backed Digital Signatures into evidence as part of the Massachusetts Legal Hackers practice mock trial walk through on July 12th at 6:45pm at the MIT Media Lab.

In the course of a breach of contract suit, the attorney wishes to introduce a computer printout that sets forth the date, amount, payee and purpose of a payment issued by 123, Inc. in order to show that 123, Inc. made a payment to Alice Arlington in purchase of her used car. This sample

[1] Michelle L. Querijero, Esq., *Documentary Evidence §9.17: Foundation*, Shipman & Goodwin LLP 33–34 http://www.shipmangoodwin.com/files/19628_Chapter09Final.pdf (last visited July 12, 2017).

dialog demonstrates the introduction of that printout and assumes that counsel will be required to show the reliability of the process that produced the printout.

> *NOTE: This draft is adapted from the sample examination contained in the background reading below (see: § 12.4.7 Sample Examination) but this may not be a desirable or even workable witness examination approach for the purpose of revealing the likely evidentiary issues raised by this technology. One notable complexity with the approach is that it assumes a business is one of the parties and that the business is large enough to have technology staff. One implication of assuming a sizable business as one party in litigation is that the scope and circumstances of the underlying fact pattern may become too complex and hence burdensome to be realistically simulated within the time and resources proportional to this exploratory and relatively informal activity. Experienced litigators and others with expertise in the field of evidence are welcome and encouraged to offer modified or completely different approaches.*

ATTORNEY: Please identify yourself, stating your occupation and place of employment.
WITNESS: My name is Linda Green, and I am the director of data and applications for 123.
ATTORNEY: How long have you held that position?
WITNESS: Since January 2012.
ATTORNEY: What are your responsibilities as the director of of data and applications?
WITNESS: I am responsible for the collection, organization, maintenance, and dissemination of all data used by 123 in the regular course of its business.
ATTORNEY: Are you familiar with cryptographic digital signature?
WITNESS: Yes.
ATTORNEY: What are they?
WITNESS: They are [define]
ATTORNEY: Does ABC, Inc. make use of cryptographic digital signatures?
WITNESS: Yes, since June 2017, 123 has used cryptographic digital signatures.
ATTORNEY: Are you personally familiar with the application and processes used by 123?

WITNESS: Yes. I was responsible for our selection and deployment of the application used to generate, store, share and verify the digital signatures and I have participated in the design of all software projects currently in use by 123.

The witness then describes, in answer to a series of questions, the application and its capabilities, including how the application uses standard Bitcoin core wallet and signing libraries to generate a cryptographic key pair and public blockchain address for each user, as well as the particular workflows that replaced 123's prior email-confirmation based electronic signature method.

ATTORNEY: Are the blockchain ledger and signature application systems you have just described used in the regular course of 123's business?
WITNESS: Yes.
ATTORNEY: Is it the regular course of business of 123 to store copies of all digitally signed data executed by this application on a server physically located at your office and also on a cloud backup you host on Amazon Web Services?
WITNESS: Yes.
ATTORNEY: Who at 123, Inc. is responsible for managing the backup process for signature data?
WITNESS: John Brown, 123's chief financial officer, and his two assistants, Mary Conto and Tim Armana.
ATTORNEY: Are you familiar with the manner in which such data is collected and stored in the the local data server and cloud backup?
WITNESS: Yes.
ATTORNEY: Please describe the way in which it is done.

The following remains to be drafted:

- Witness describes the
    - procedures used to back up the signature data
    - process by which the application cryptographically signs a digital document or other data

- practices and logged workflow events used by 123 to link customers (identifiable legal parties) to cryptographic key pairs used by the application
- program and API used by 123 to enter hashes of all digitally signed data generated each day, week and month onto a public blockchain (eg: https://tierion.com/docs/hashapi)
-

ATTORNEY: Your Honor, I offer the printout into evidence as Defendant's Exhibit 2.
OPPOSING COUNSEL: Objection.
JUDGE: Objection overruled. The printout is [...admissible...].

ATTORNEY: Linda, what is the document that has been marked as Exhibit 2?
WITNESS: 123, Inc.'s purchase agreement for Alice's used car.
ATTORNEY: Is the purchase agreement kept in the regular course of business by 123?
WITNESS: Yes.
ATTORNEY: What is the date of the agreement?
WITNESS: [date]
ATTORNEY: How much did 123 agree pay for Alice's car based on the agreement?
WITNESS: [state amount]
ATTORNEY: Who signed the agreement on behalf of 123?
WITNESS: I did.
ATTORNEY: Does the agreement state that you signed it?
WITNESS: Yes.
ATTORNEY: How do you know that you signed it?
WITNESS: Because of my cryptographical signature right here.
ATTORNEY: Did Alice sign the agreement using a cryptographical signature?
WITNESS: Yes, she did.
ATTORNEY: How do you know that?

WITNESS: Because her cryptographical signature appears right here on the document.
ATTORNEY: How do you know that it was Alice who made that cryptographical signature?
WITNESS: [Explain how 123's cryptographical signature process is foolproof.]
ATTORNEY: Thank you Linda, that is all I have.

QUESTIONING OF ALICE BY ALICE'S ATTORNEY:
ATTORNEY: Good morning can you please state your name for the record?
WITNESS: Alice Arlington.
ATTORNEY: Where do you reside?
WITNESS: Cambridge, MA.
ATTORNEY: Do you know 123, Inc.?
WITNESS: Yes.
ATTORNEY: What is it?
WITNESS: A car dealership.
ATTORNEY: Have you ever been there?
WITNESS: Yes, I have?
ATTORNEY: Why did you go there?
WITNESS: I was considering selling my car to them.
ATTORNEY: Did you?
WITNESS: No.
ATTORNEY: Who did you speak with at 123?
WITNESS: A woman named Linda?
ATTORNEY: What did you speak about?
WITNESS: I showed her my car and we talked about how much it was worth and whether 123 would buy it from me.
ATTORNEY: Did 123 make you an offer?
WITNESS: Yes.
ATTORNEY: Did you accept the offer?

WITNESS: I thought about it and we went over some paperwork but ultimately I chose not to sell it to them.
ATTORNEY: So you never signed any paperwork with 123?
WITNESS: No I didn't.
ATTORNEY: Thank you Alice that is all I have:

123's ATTORNEY's CROSS of ALICE:
ATTORNEY: Alice, please look at Exhibit 2. Does your cryptographic signature appear on this agreement?
WITNESS: I don't think so.
ATTORNEY: Well, your name appears towards the bottom of the agreement, doesn't it?
WITNESS: Yes it does.
ATTORNEY: No further questions your honor.

[Should there be a short closing argument by the attorneys where they summarize the important evidence that establishes (or does not establish) a valid signature/agreement]

-------- END ------

Next Steps from July 12 2017 Meeting:

- Update Witness Examination to hone the basic descriptions of the technology
- Tighten fact pattern and narrow scope of relevant legal content to specific key issues impacting evidentiary (especially admissibility) requirements. The Federal Rule 901 six criteria relating to technology evidence is a good start.
- Prepare a complete walkthrough for next session (a dress rehearsal in Mock Trial courtrooms where the final event will be held), including: complete script of all roles and the specific objections and rulings; the physical exhibits to be entered into evidence (we decided paper printouts of the files with signature information) and if possible, some props of some type to help illustrate the technology to make it understandable.
- Document key requirements, constraints or high-value priority features revealed from the process of modeling and running through litigation processes,
    - Post and/or Video: Document as "lessons learned" short blog posts or project wrap up video;

    - UML and/or Issues: Document requirements/features revealed as short “use cases” or other diagrammatic models (eg UML) and/or as issues in the GitHub code repository where the digital signature application used for this Mock Trial is being developed. Express the issues as tractable, discrete and measurable tasks linked back to the requirements, constrain or other priority revealed through the Mock Trial process (eg linked to a specific rule of evidence or judicial rule or perhaps a practical need identified through the process)
- Convene a Google Hangout for further iteration of above to prep for dress-rehearsal and also one or more informal Meetups at Code for America Tuesday “Hack Night”

Potential Vectors of Attack: Grounds for Objections/Defenses

Authenticity of the Evidence

The evidence is not sufficient to attribute the digital signature to the party who purportedly executed the signature

- The key pair used to execute the digital signature is not the same as the key pair associated with the signer (demonstrate by comparing the public key or hashed public key blockchain address purportedly attributable to the signer with the actual key or address of the signer to show they are different)
- The key pair is associated with the purported signer but was not applied to the document in question (demonstrate by use of SHA 256 message digest comparison)
- The implementation of the cryptographic and related technology by the digital signature application was so flawed that there is no reasonable basis for attributing the signature to the purported signer or even to the transaction (demonstrate by highlighting the relevant log or ledger entries or associated metadata to spotlight that the information is not genuine or authentic.
- The record of the transaction asserted to have been entered onto a given public blockchain is different from the data as it exists on the current consensus based distributed ledger or public blockchain in question (demonstrate by comparing the hashes on the block on which the transaction in question is asserted to have been entered is provably incorrect by hashing the block and demonstrating the hash result (eg the SHA 256 message digest for the data comprising that block) is different from the hash digest explicitly entered for that block.
-

Relevance of the Evidence

The date/time of the signature relates to a different transaction or activity

- The digital signature was created so far before or after the date/time in question it is not relevant to the transaction being litigated (demonstrate by use of application generated date stamp if we have that, or by entry of the signature or hash of signed document onto Bitcoin or Ethereum public blockchains)

The date/time of the signature corresponds to the transaction or activity being litigated but document is irrelevant to the matter

- The document that the signature was applied to was not the contract itself although it was signed by the key pair of the purported signer and at the relevant period of time

Lack of Direct Knowledge

The witness was not the purported signer and lacks direct knowledge of the signing event

Lacks General Acceptance by Scientific Community

This objection could be appropriate if the party seeking to enter the digital signature into evidence makes a motion requesting Judicial Notice of blockchain technology or requesting information entered onto a public Blockchain to be considered self-authenticating

- Blockchain technology is not generally accepted by the scientific community, even if aspects of the cryptography, hash algorithms, distributed computation and other technologies are individually accepted the entirety of the system is novel and not yet generally accepted
- Blockchain technology should not be accepted as backed by general science due to the difficulty disentangling the “hype” and resulting uncertainty about claims and assertions shrouding whatever benefits or reliable capabilities the technology might provide.

Attack Security Flaws of the Implementation

- Even is the math and crypto is strong the implementation is subject to challenge.
    - Security flaws from the softwar

_____

General Running Notes and Observations (The Parking Lot)

Is the use of expert testimony required in order to do an initial walk through intended to reveal the likely key evidentiary issues. Is there a credible and useful model of routine litigation by parties such as small businesses or individuals that is somewhat above the dollar thresholds for small claims court but pursued by parties who may lack the resources to engage expert witnesses?

What props or other tangible artifacts can and should be used to explain the evidence?

What artifact would be entered into evidence - a disk?

- Digital information delivered by way of authorized electronic court filing (eg as is done for pleadings, motions, etc)?
- A print out of the application UI showing the result of purported signature verification (green check mark, etc)?
- Print out of the underlying key data points (eg: the document that was signed, the signature block and the hash digest of the signed document)?
- Other?

If a print out of the file that was signed and the hash of the contract document is to be entered, then must the electronic record instantiating the contract have been a plain text file or markdown file encoded in a format such as UTF-8? Otherwise, if the file that was digitally signed was in PDF, MS Word or other such format, would the printout need to be something like the hex or octets that were actually signed? If the raw data is printed and entered into evidence in machine readable but not human readable form, what is the purpose of printing it in the first place?