From: Sai
Sent: Friday, April 09, 2021 6:30 AM
To: RulesCommittee Secretary
Cc: elizgib
Subject: Re: FRBP pro se electronic signatures & CM/ECF

As a further comment — and suggestion:

Regarding the supposed security of "wet" signatures, which was a premise of several arguments made during the FRBP meeting: that premise is false, and the arguments from it are therefore invalid.

I suggest to the committee that the entire idea of traditional "signatures", especially ink signatures, is obsolete. In its place, the courts should adopt decades-old concepts from computer security.

All that really matters is
1. identification ("who is this person");
2. authentication ("how do I know the person doing this action is who they say they are"); and
3. authorization ("what is the identified person allowed to do").

These are not just computer security terms; they are also the
controlling legal questions.

Whether someone physically signed a piece of paper is barely even relevant, legally. What matters is:
* who someone is;
* whether they intended to agree to a given document (or file it, swear to it, or whatever else the document says);
* whether they were authorized to agree to it;
* whether the document one is looking at is the one that was agreed to; and
* proving all those things.

Ink signatures do exactly none the above.

Images of the handwritten signatures of many famous people are easily available online. The "ink" signatures of judges are often in the PDFs they sign, and are trivial to extract and insert into other documents. Its presence proves very little.

"Wet ink" signatures by a pen cannot be distinguished from a color printer, short of forensic analysis with a spectrograph, which courts don't do. Why demand something you can't even distinguish?

Even for a recluse, it's often nearly impossible to actually tell whether one ink signature is from the same person as the last. People change their signatures over time, and a lot have basically the same sawtooth scribble as their "signature". An X is a legal "signature". Have clerks become handwriting experts?

Electronic filing proves exactly one thing: that the document was

filed by someone who, at time of filing, has access to the account credentials of the person who registered for that account.

It doesn't prove that the document was actually filed by the attorney of record to whom the account is registered.

In fact, current civil rules do not even *allow* an attorney to designate another account (e.g. their paralegal) as being authorized to file on a given case. (I don't know whether the same is true of FRBP.)

Instead, courts tell filers that if they want to authorize someone else to file for them, they should share their personal CM/ECF username and password with the other person.

This is alarmingly bad security practice. *Nobody* should ever know your personal passwords, and the courts should not encourage this.

Instead, the courts should allow one account to authorize another account to perform certain actions on its behalf — for instance, an attorney authorizing their paralegal to make filings for them. This authorization could be restricted — e.g. to specific case(s) or even specific types of filing (e.g. perhaps allowing a paralegal to file less sensitive things, like motions for extension, but not more important ones, like a stipulation of dismissal or motion for summary judgment). The filer can then withdraw that authorization later (e.g. if the paralegal leaves), or extend it (e.g. if they are assigned to a new case), without ever having to share or change their personal account credentials.

This would also make exact attribution, auditing, etc much clearer in case there is later any issue with needing to determine who actually filed the document.

I note that this is in fact the system that is already in place for judges (more or less). Court orders are routinely filed on CM/ECF by judges' law clerks, clerks of court, etc. — not personally by the judge.

ECF docketing properly reflects that. The person actually filing is named on the docket as the filer (e.g. showing the initials of the docket clerk handling the case at the end of the docket entry), whereas the document itself shows the person under whose authority the document is made, e.g. the judge.

The same should apply to all other filers — both attorney and pro se.

For any given document, it should be clear:
a) who actually signed in to CM/ECF and filed the document
b) who authorized the document to be filed
c) who authenticates or agrees to the content of the document
d) on whose behalf the authorizer is acting

It is not unusual that these are all different people. Consider, for instance, filings made by DOJ — USA, AUSA, line attorneys, witnesses, paralegals…

As for all electronic signature services — including CM/ECF and its sign up process itself, which *is* an electronic signature service — the exact same questions apply as I stated at the outset.

Your acquiescence to CM/ECF, and its sign up process, has created an estoppel. You cannot demand that pro ses go through more rigorous security — e.g. notarization or ID checks on signup, let alone on every filing — than you agree is acceptable for CM/ECF.

That, therefore, is the standard of comparison.

Applying principles, the questions before you are:

1. Does the system verify the applicant's identity as much as, and no more than, the CM/ECF signup form?
2. Does it verify that they are the same person as the one who signed up as much as, and no more than, a CM/ECF username and password?
3. Does it verify that the person with that account is authority to submit the filing in question as much as, and no more than, CM/ECF?

If yes, approve it. If not, reject it.

And please don't lock pro ses into a single system, unless it's CM/ECF itself; that would create an exploitative monopoly, as we see routinely in prison "services". If it passes, it passes. Markets don't work without competition.

The above comments and suggestion are submitted based on my expert opinion as a computer security professional with significant experience in using, taking apart, defending, attacking, and designing systems that must be very careful about exactly what proves what — including signature, authentication, and identity validation systems.

See https://s.ai/work/legal_resume.pdf

Sincerely,
Sai

Sent from my mobile phone; apologies for autocorrect errors and concision