Electronic Signatures vs. Digital Signatures and Understanding Identity Repudiation

Tim Sullivan
ActivePDF, Inc.

ActivePDF

Why are you here?

1. Wait…isn't a signature a signature?
2. What's the difference and why should I care?
3. What the heck is identity repudiation?
4. Am I at risk?
5. Should I build or buy?
6. I've got questions!

Electronic Signatures

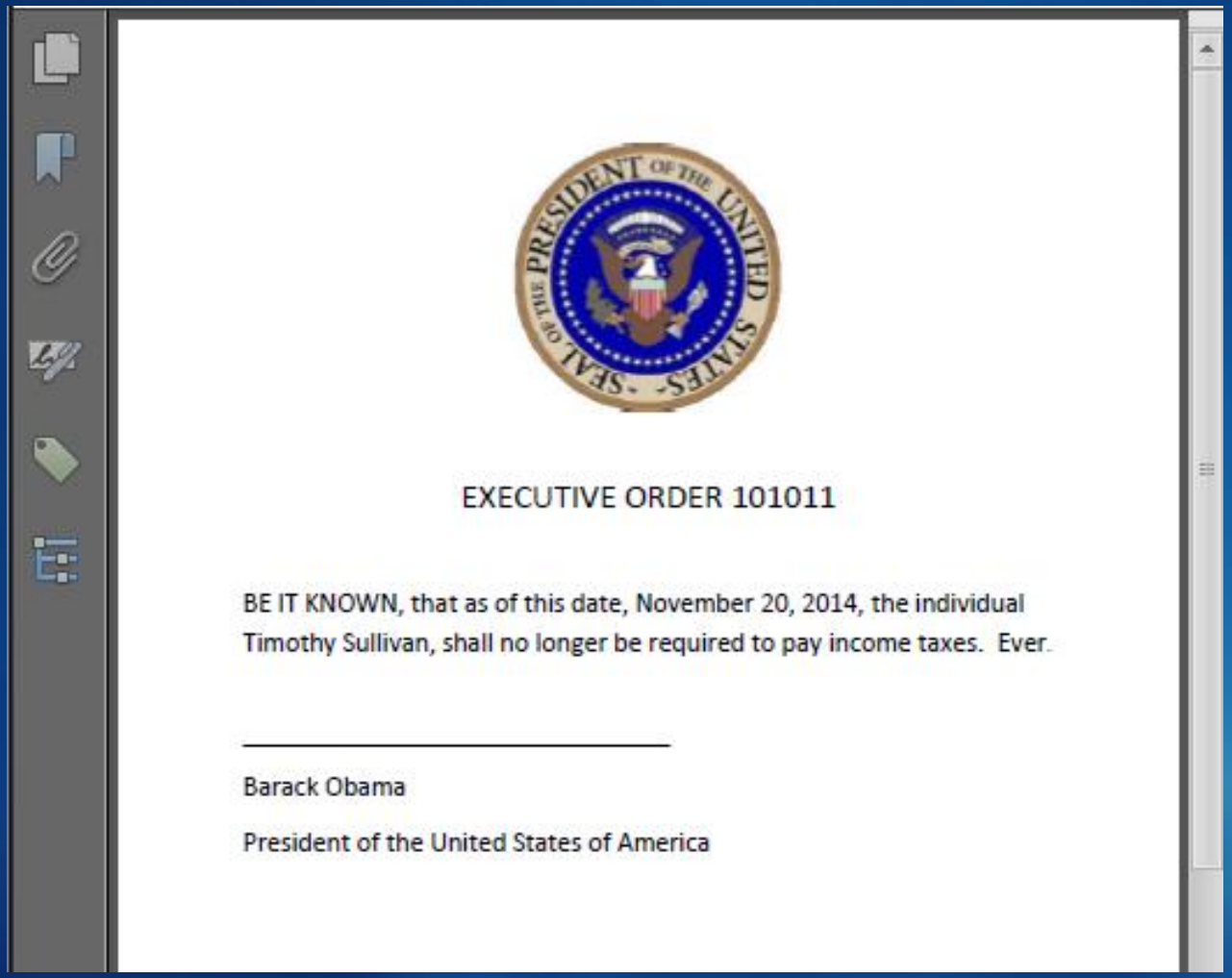
- ESIGN Act of 2000 - 15 USC 7006 (5) – The term “electronic signature” means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

- Contains other provisions for storage, reproduction and electronic consent.

- There is **nothing** in the Act for establishing identity of the signer (or even the integrity of the record). In fact, the Act puts limitations on the agencies to require the use of specific technologies.

Electronic Signatures and PDF

Before



EXECUTIVE ORDER 101011

BE IT KNOWN, that as of this date, November 20, 2014, the individual Timothy Sullivan, shall no longer be required to pay income taxes. Ever.

_____

Barack Obama

President of the United States of America

ActivePDF

Electronic Signatures and PDF

After insertion of PNG file

EXECUTIVE ORDER 101011

BE IT KNOWN, that as of this date, November 20, 2014, the individual Timothy Sullivan, shall no longer be required to pay income taxes. Ever.

Barack Obama

President of the United States of America

ActivePDF

Good Enough?

- In some cases (which we will touch on later) it might be, but by itself, no.
- It's difficult to prove the "intent" required under 15 USC 7006 (5).
- How can you prove the identity of the signer?

Digital Signatures

- A mathematical scheme for demonstrating the authenticity of a digital message or document.
- A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message and that the message was not altered in transit.
- (source : http://en.wikipedia.org/wiki/Digital_signature)

Digital Signatures (for the layperson)

- Everything (characters, images, etc) in the document are pumped through a “process” to create what we will call a “magic number”.
- Any change to the document alters the magic number.
- The magic number is then “locked” with a private key (PKI…more on that in a moment) and stored inside the document or logically associated with the document.
- The magic number can be “validated” with a public key.

Digital Signing Process

ActivePDF

PKI (for the layperson)

- PKI – Public Key Infrastructure and also known as asymmetric cryptography
- There are two keys – The public key that you can give away and the private key that you hold near and dear to you.
- With PKI – One key can ONLY either lock or unlock and the other key can ONLY do the opposite.

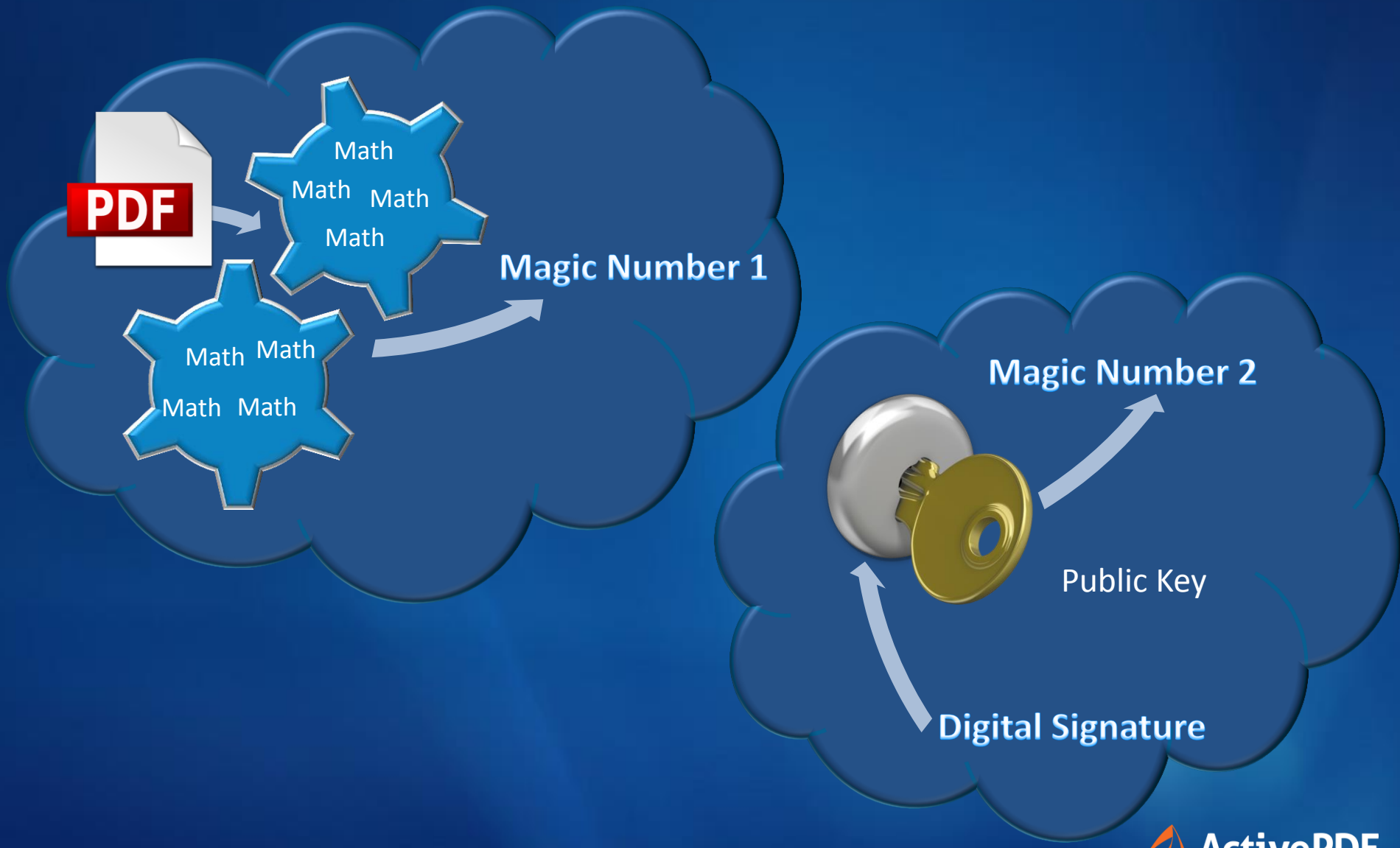
PKI vs Traditional Passwords

Traditional password – symmetric cryptography

PKI vs Traditional Passwords

PKI – Asymmetric cryptography

Digital Signature Verification



ActivePDF

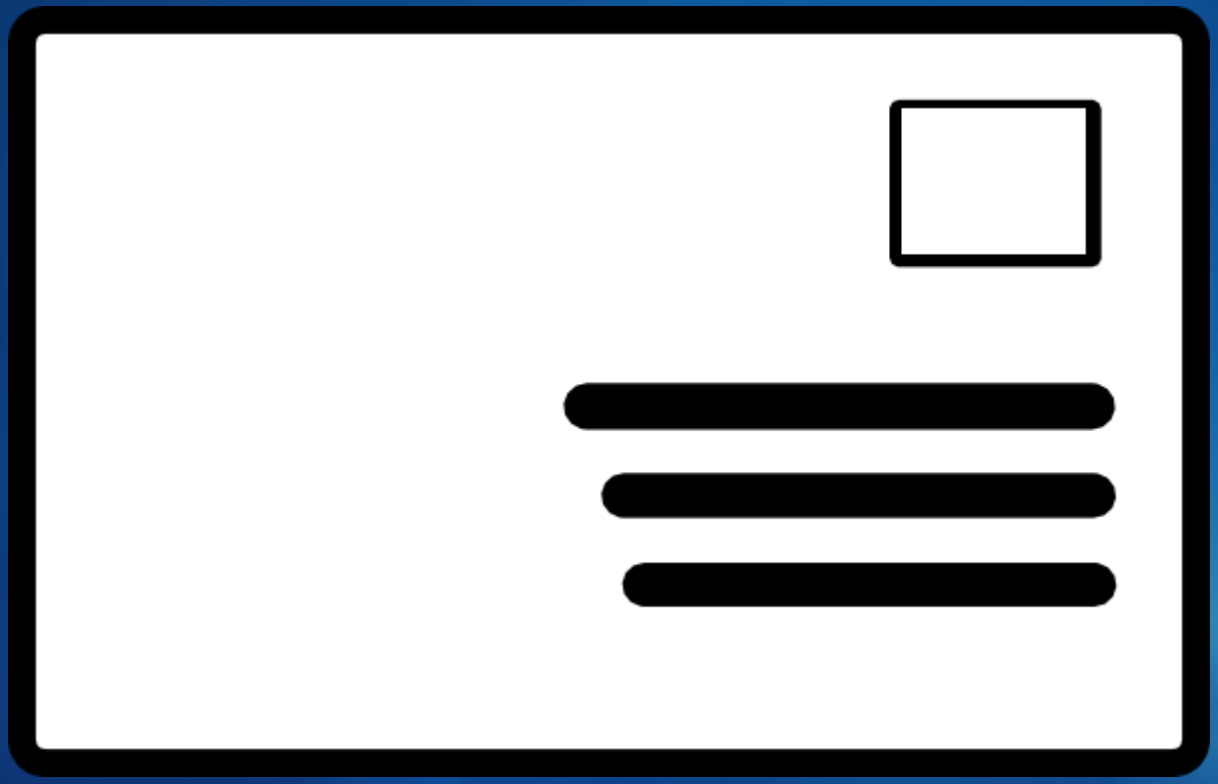
Digital Signature Verification

IF

Magic Number 1 = Magic Number 2

ActivePDF

Digital Signatures in PDF



ActivePDF

Digital Signatures in PDF

Digital Signatures in PDF

ActivePDF

Digital Signature + E-Sig = Best Practice

- If I only supply a Digital Signature is the definition of the “electronic signature” requirement of the ESIGN act satisfied?
- The short answer – Yes. A Digital Signature is a process under the ESIGN act.
- The long answer – We tend to associate a “signature”, whether our own or computer-generated, with acceptance, so having both a visual electronic signature and a digital signature is the best practice.

Digital Signature vs E-Signature or Why do I care?

- Contract enforcement
- E-Discovery
- Litigation

While a document under the ESIGN Act is given the same legal weight as a “wet copy”, you may still have foundational issues to overcome. When, where, how and most importantly…WHO.

What is Identity Repudiation?

I don’t believe you are who you say you are and you didn’t actually sign this document.

(aka I don’t Trust You)

Or

I didn’t sign that document

and you need to prove it.

(aka You can’t Trust Me)

Establishing Identity

Outside the document

- Personal relationship
- Communicated intent
- Organizational association
- Execution

Inside the document

- Geolocation
- IP Addresses
- Two way authentication
- Embedded intent
- Personal identifiers
- Email verification
- 3rd party verification (eg personal public key)

The Trust Versus Risk Continuum

Trust is inversely proportional to risk.

The lower the trust, the higher the risk.

The higher the trust, the lower the risk.

Weighing Risk

Examples of High Risk

- Anonymous user
- Direct from website
- One on one verbal communication
- Unverifiable data
- Single transaction
- Execution precedes payment

Examples of Low Risk

- Met personally
- Email communications
- 3 party telephone calls
- IP Address can be tied to company
- Validated credit card information
- Previously established authentication
- Payment precedes execution

Build vs Buy
Using A 3rd Party to Establish Trust

Party A

1. Party A and Party B establish a relationship and a decision to execute a document is made.

Party B

3. Party A requests Party B through Party C to sign the document.

2. Party A authenticates with Party C and submits the document for signature.

Party C

4. Party B signs the document with Party C and Party C retains a copy for both parties to access.

ActivePDF

3rd Party Provider Benefits

- Authentication of the sender
- Authentication of the receiver
  - Email link
  - Two factor authentication
- Trusted digital certificates
- Platform independent technology to visibly sign
- Timestamp signing
- Import form and convert to PDF
- Design forms
- Signed document archival
- Logging of activity
- Trusted names in the industry

3rd Party Providers

- DocuSign
- EchoSign (Adobe)
- NitroCloud
- RightSignature (Citrix)
- SignNow (Barracuda)

You can build it though!

- A good alternative if trust is HIGH
- If signatures are in a fixed location or easily identified by a PDF field name otherwise you will have to build a designer
- Plenty of third party products that can preview a PDF, insert signature images and digitally sign a PDF
- You can use “trusted” digital certificates from Verisign, Thawte, etc. or be your own “certificate authority”
- You can use your own existing authentication to confirm identity (e.g. Active Directory, Open ID, custom database)

If you build it, you must also…

- Provide a consent mechanism
- Audit trail all activity of the signing process
- Make the signed document accessible to all parties for periods as determined by statute, regulation or rule of law
- Document the entire process to make sure it meets ESIGN requirements
- Of course, weigh the costs against the risks.

Questions?

Thank you!

Email: tim.sullivan@activepdf.com

ActivePDF