

Interagency Advisory Board

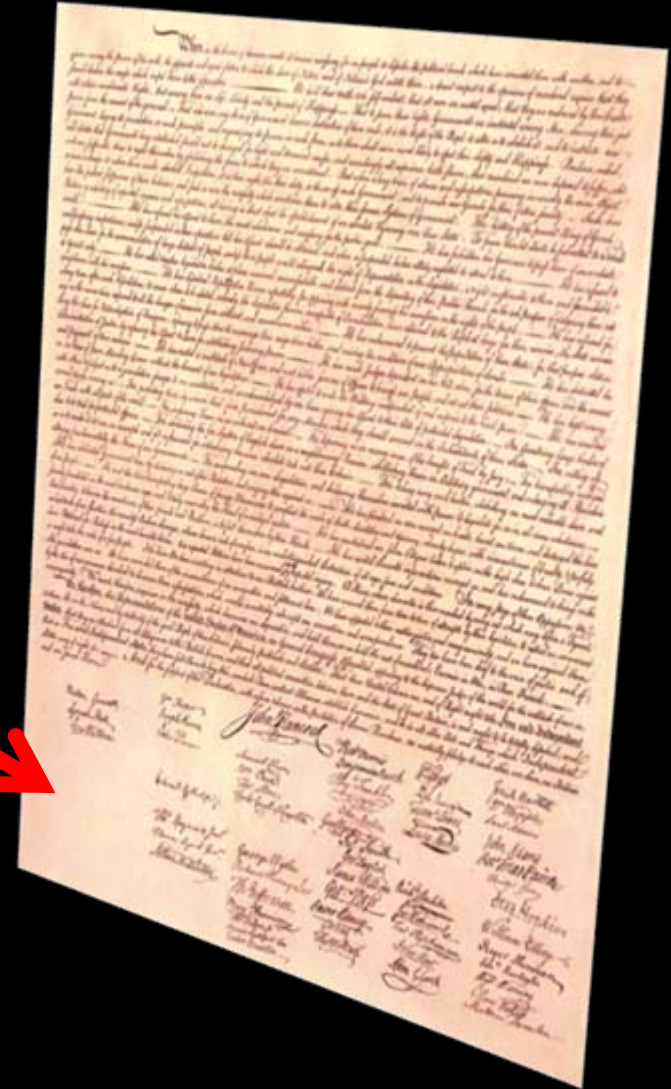
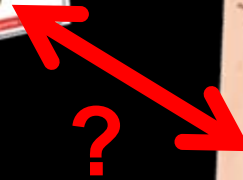
Meeting Agenda, January 27, 2010

1. **Opening Remarks**
2. **Digital Signature Lessons Learned** (*John Landwehr, Adobe*)
3. **Challenges of IdM for the Virtual Lifetime Electronic Record (VLER)** (*Doug Felton, DoD/VA Program Office*)
4. **Global Threat Intelligence** (*Phyllis Schneck, McAfee*)
5. **New Initiative- Joint IAB/SCA Meetings** (*Randy Vanderhoof, Smart Card Alliance*)
6. **The Value of PKI** (*Judy Spencer, GSA*)
7. **Closing Remarks**

Digital Signatures

John T. Landwehr,
CISSP
Director, Security Solutions
Adobe Systems Incorporated

January 27, 2010
@IAB



Why “Signatures”?



A signature (from Latin *signare*, "sign") is a handwritten (and sometimes stylized) depiction of someone's name that a person (“signatory”) writes on documents as a proof of identity and intent.



Used for:



1. Providing evidence to provenance/identity/status of the document

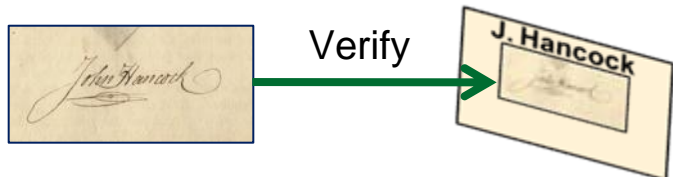


2. Acknowledging informed consent / approval by the signatory

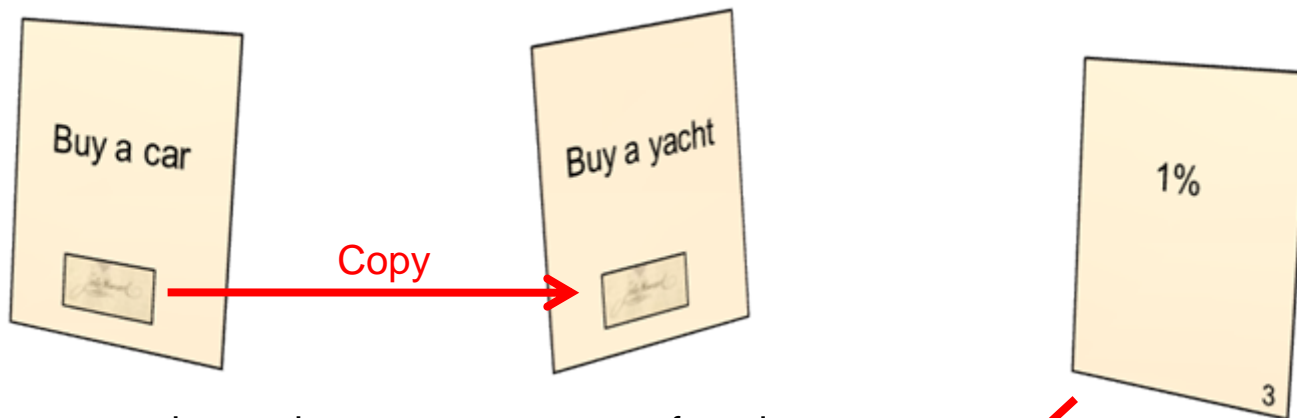
3. *Philography*

Challenges with paper signatures

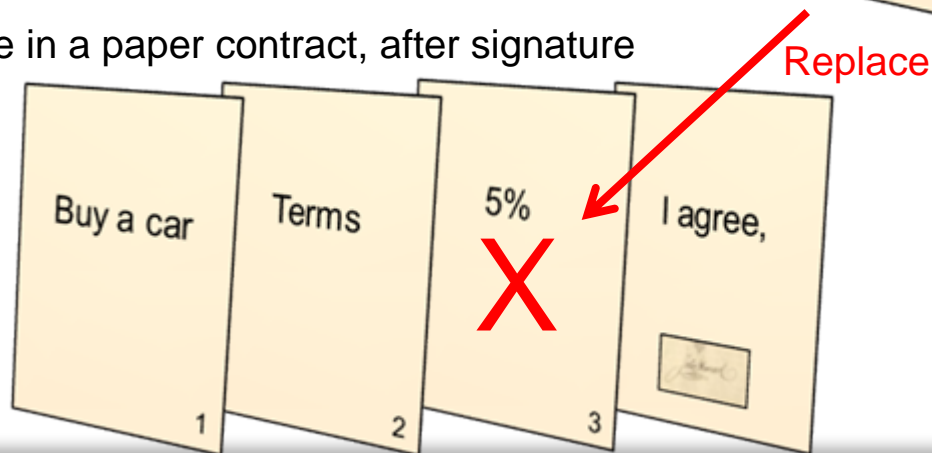
1. Need to compare with a valid source (e.g. the bank signature card on file)



2. After seeing any signature, unauthorized reproductions are possible



3. Content can change in a paper contract, after signature

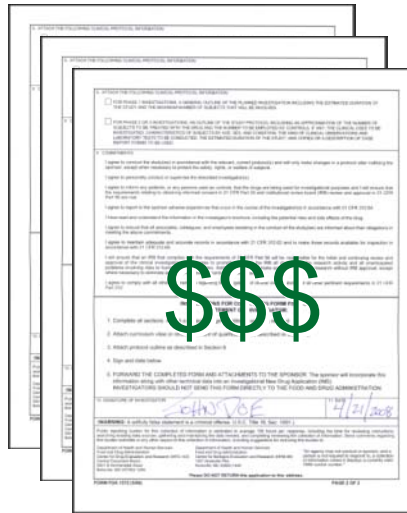


An ink signature is fast & cheap – consumables, delivery, storage and authenticity are not...

10¢

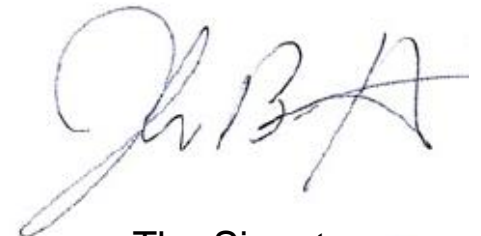


The Pen

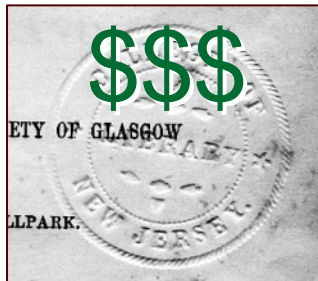


Toner & Paper

2sec



The Signature



Authenticity
Paper/Ink/Seal



Storage



Courier / Delivery/Fax

The cost extends beyond monetary budgets



- Every 9000 printed pages = 1 Tree
- Nearly 4 Billion trees worldwide are cut down each year for paper
- Paper production utilizes significant energy and water supplies

The migration to all-digital workflows requires eSignatures

Generation

Agency

Delivery method

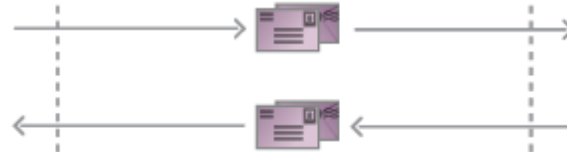
Customer

First

traditional paper-based delivery



form retrieved from archive,
mailed to customer



customer fills and signs form,
mails back to agency

Second

hybrid electronic delivery



form archived as pdf, accessed
through portal, pdf delivered by
e-mail or download



customer prints, fills, and signs form, mails
back to agency

Third

pure electronic delivery and submission



form archived as pdf, accessed
through portal, submitted with
prepopulated information fields

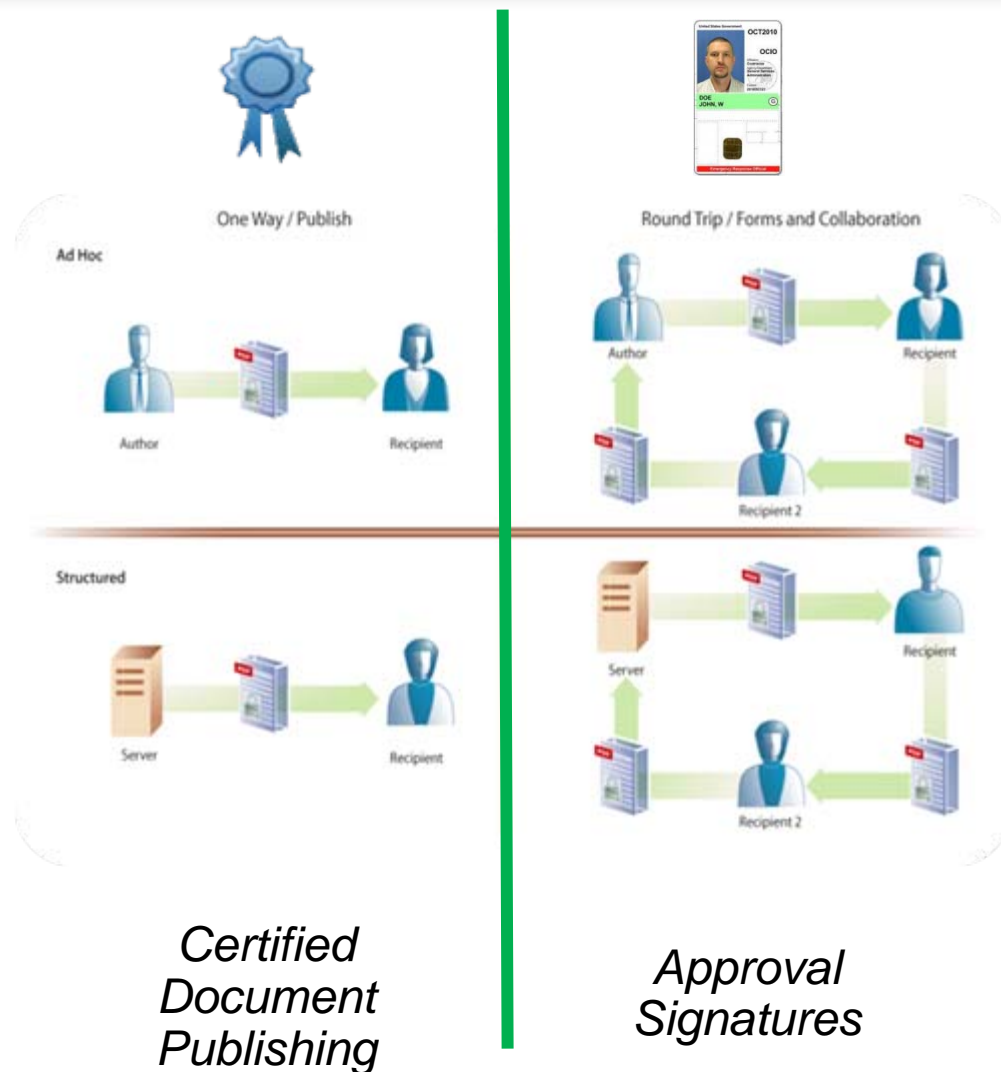


digitally fills and signs form, submits
secure, certified pdf to agency

<All digital, all the time>

Benefits of electronic signatures

- Faster, cheaper, more secure, and more environmentally friendly than paper signatures
- Binds signatory identities to document
- Mitigates signature copying
- Mitigates document forgery
- Signatures are still visible “on document”
- Human & machine-readable
- Numerous technical standards well established

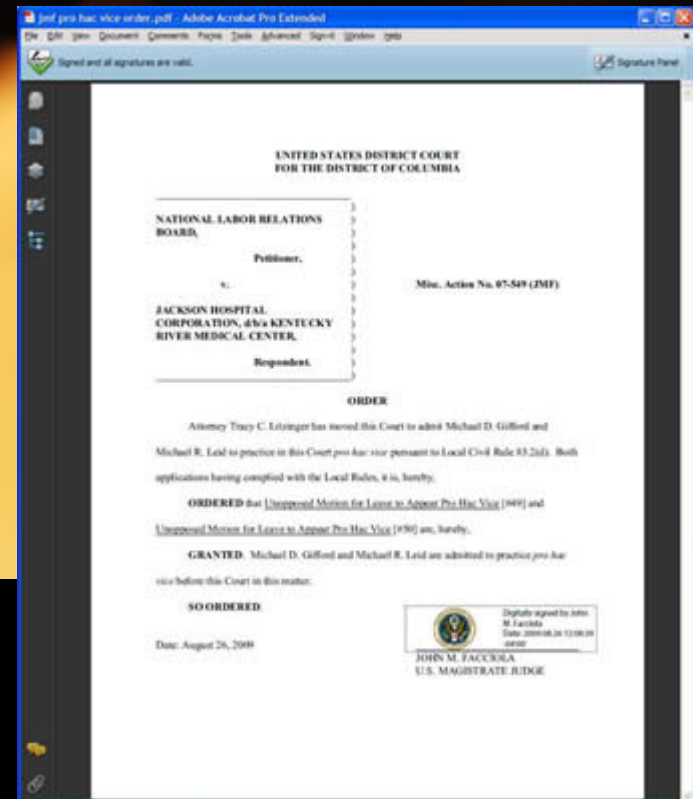


“Are electronic signatures legal?”



Honorable John M. Facciola,
Magistrate Judge for the U.S. District Court
in the District of Columbia
signing a judicial order in PDF

courtesy of National Notary Association
August 26, 2009



Where do they get the PKI for a digital signature?

- Some countries with ID cards containing signature certificates:
 - Austria, Belgium, Estonia, Finland, Iceland, Italy, Malaysia, Portugal, Saudi Arabia, Spain, Sweden, UAE
- Some of their common applications:
 - Healthcare, Tax/VAT, social security, childcare, criminal reports, business registration, disability programs, marriage licenses, patents, Internet voting, driver and vehicle registration, real estate, general egov forms
- Other commercial and government organizations deploy software and hardware certificates (card, USB token)



Examples: Citizen approvals

Argentina National Social Security Administration



- Forms
- Pension, retirement

Land Title & Survey Authority of British Columbia



- Property titles, surveys
- Legal submissions

Government of Italy



- Forms
- Benefits Delivery
- Various agencies

Government of Belgium



- Forms
- Benefits Delivery
- Taxation

Examples: Internal Process Approvals

This authorization will remain in effect until you notify the applicable Department of Defense cancellation.

In consideration of the privilege of having the U.S. Treasury initiate debit and credit transactions specified above, I hereby freely and voluntarily consent to the immediate collection from Marine Corps or Army, without prior notice or prior opportunity to be heard, the face value or balance due the U.S. Treasury funds pool of any funds which were transferred to my Navy/Military union account because a transaction is dishonored and returned for insufficient funds, closed information, or any other return reason.

27. SIGNATURE



A handwritten signature in black ink that reads "John".

Digitally signed by John Landwehr
Date: 2008.03.07 10:00:18 -08'00'

Procter & Gamble

- R&D Records
- Approvals
- Submissions to FDA



US District Court - DC

- Judicial Orders



Large NJ Book Publisher

- Internal approvals
- Travel requests
- Expenses



Examples: Certifying Documents

US Government Printing Office

- Federal Budget
- Public Laws
- Government Documents



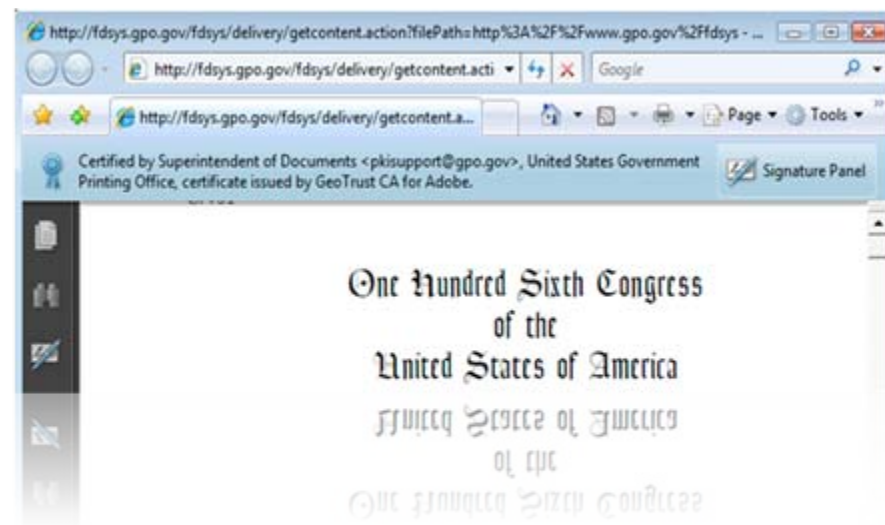
Avow Systems

- E-transcripts
- Higher ed



Antwerp Port Authority

- E-Invoicing
- Compliance



What some organizations have said...



- Internal Forms/Processes:
 - Procter and Gamble saves \$ millions / year
 - Bell Alliance law firm saves 100s of hours per month in customer transactions
 - Pfizer saves \$125 per digital signature
- Government Services:
 - Land Title & Survey Authority of British Columbia saves \$50/transaction with total savings of over \$300K/year for LTSA plus \$100Ks for law firms
 - Argentinean Social Security Administration (ANSES) achieved ROI in 24 months , eliminated delays and errors in citizen forms, and significantly improved response times

Electronic Signatures provide... Environmental Sustainability



- Publishing: GPO to save 20 tons of paper over 5 years with PDF budgets
- Internal Forms / Processes: P&G saved 2.5M sheets of paper

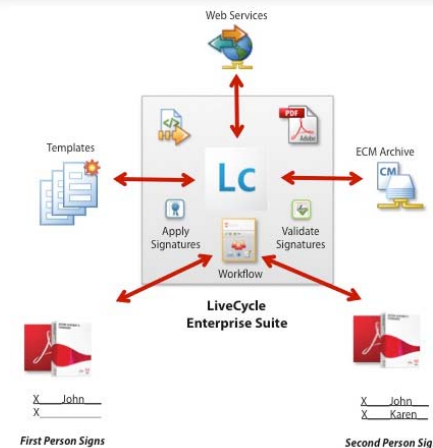
Adobe Digital Signatures in PDF



**Acrobat and Reader
JITC Certification**

NLST

**FIPS 140-2 modules
for AES/RSA/SHA
PKITS for Path Validation**



Automated Workflows

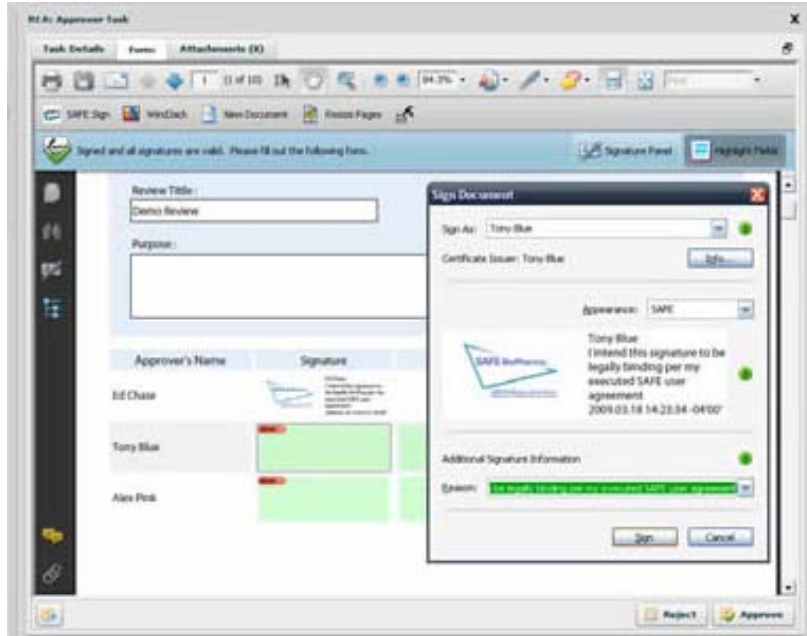
- Cross Platform
- CDS / AATL Trust Framework
- PDF = ISO Standard
- CRL and OCSP
- RFC 3161 Timestamps
- Long Term Validation
- XML Signatures

Other Good Stuff



**Smartcard support
CAPI & Keychain**

Tips & Tricks



- Use seed values in form authoring
- Use MDP+ for multi-signature forms
- Use OCSP – avoid CRLs
- Embed revocation when signing
- Automate validation on server
- Use CDS/AATL/enterprise settings
- Clearly differentiate signing cert
- Be careful with OIDs
- Review customization settings

- Adobe Security Home – **adobe.com/security**
- *Security Matters* Blog – **blogs.adobe.com/security**
- Acrobat Security Documentation –
learn.adobe.com and
adobe.com/devnet/acrobat/security.html
- Adobe Security Partner Community –
partners.adobe.com/security

E-mail address–Landwehr ...