



Adobe

Adobe Digital Signatures and Elliptic Curve Cryptography

Steve Gottwals, Ph.D., CISSP | Technical Director, Security Solutions



Adobe

Adobe Acrobat and the Explosion of PDF

400K

Mobile installs
per day of
Adobe Reader

100M

E-sign
agreements
processed

50B

PDFs opened in
Adobe products
alone in the
past year

Adobe Digital Signatures



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

This document was certified by Stanford University, Stanford University with a valid certificate issued by GeoTrust CA for Adobe.

STANFORD UNIVERSITY
OFFICE OF THE UNIVERSITY REGISTRAR
STANFORD, CA 94305-6032

Name: Wonka, Warren G.
Student ID: 09876543

Print Date: 29 Oct 2007
Academic Program: UNIVERSITY
Program: Undergraduate Matriculated
25 Sep 2006: Undeclared Undergraduate Major
Active in Drop

----- Transfer Credit -----
Applied Toward Undergraduate
Transfer Credit from Unvers
Quarter Units Posted:
Total Quarter Units Posted:
Allowable A/P transfer credit:

----- Advanced Placement -----
Applied Toward Undergraduate
2006-2007 Autumn
Advanced Placement Chemis
Advanced Placement Mathm
Total Quarter Units Posted:
Allowable A/P transfer credit:

----- Beginning of Acad -----
2006-2007 Autumn
Subject # Title
CHEM 31X CHEMIC
Boudart, M
BIUM 63 TRENDO
Callan, E. Sarz
MATH 41 CALCUL
Lacturne, M
MB 389 BIOENG
York, P. Taylor

2006-2007 Winter
Subject # Title
CHEM 33 STRUCT
Newton, A
IHUM 27A ENCOUN
Khan, K
MATH 51A LIN ALG
Newton, J
SPANLANG 10 BEBENN
de Vega, L

2006-2007 Spring
Subject # Title
CHEM 35 ORO-MG
Spinosa, H
CHEM 36 ORO-CHE
Davies, C
IHUM 27B ENCOUN
Khan, K
PWR 1 WRITIN
Aristoteles, A

----- End of Transcript -----
CLICK ON SUBJECT

FISCAL YEAR 2015
BUDGET
OF THE U.S. GOVERNMENT

S. 761

One Hundred Sixty Congress
of the
United States of America
AT THE SECOND SESSION

Began and held at the City of Washington on Monday,
the twenty-fourth day of January, two thousand

An Act
To facilitate the use of electronic records and signatures in interstate or foreign
commerce.

Be it enacted by the Senate and House of Representatives of
the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.
This Act may be cited as the "Electronic Signatures in Global
and National Commerce Act."

**TITLE I—ELECTRONIC RECORDS AND
SIGNATURES IN COMMERCE**

SEC. 101. GENERAL RULE OF VALIDITY.

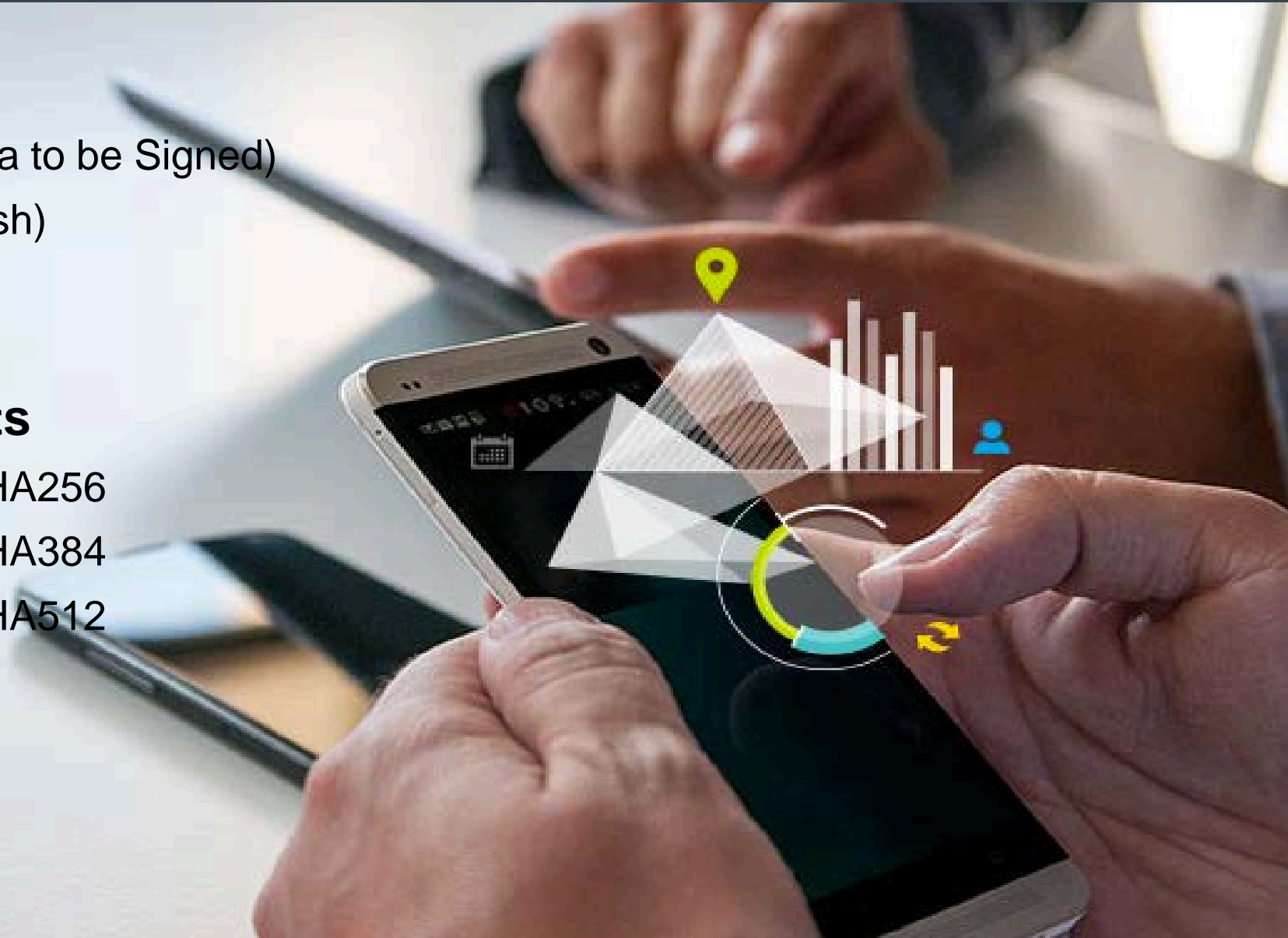
(a) IN GENERAL.—Notwithstanding any statute, regulation, or
other rule of law (other than this title and title II), with respect
to any transaction in or affecting interstate or foreign commerce—

- **Digital Signatures**

- One-Way Hash Function (Data to be Signed)
- Public Key Cryptography (Hash)
- Historically RSA, DSA
- ECDSA has Emerged!

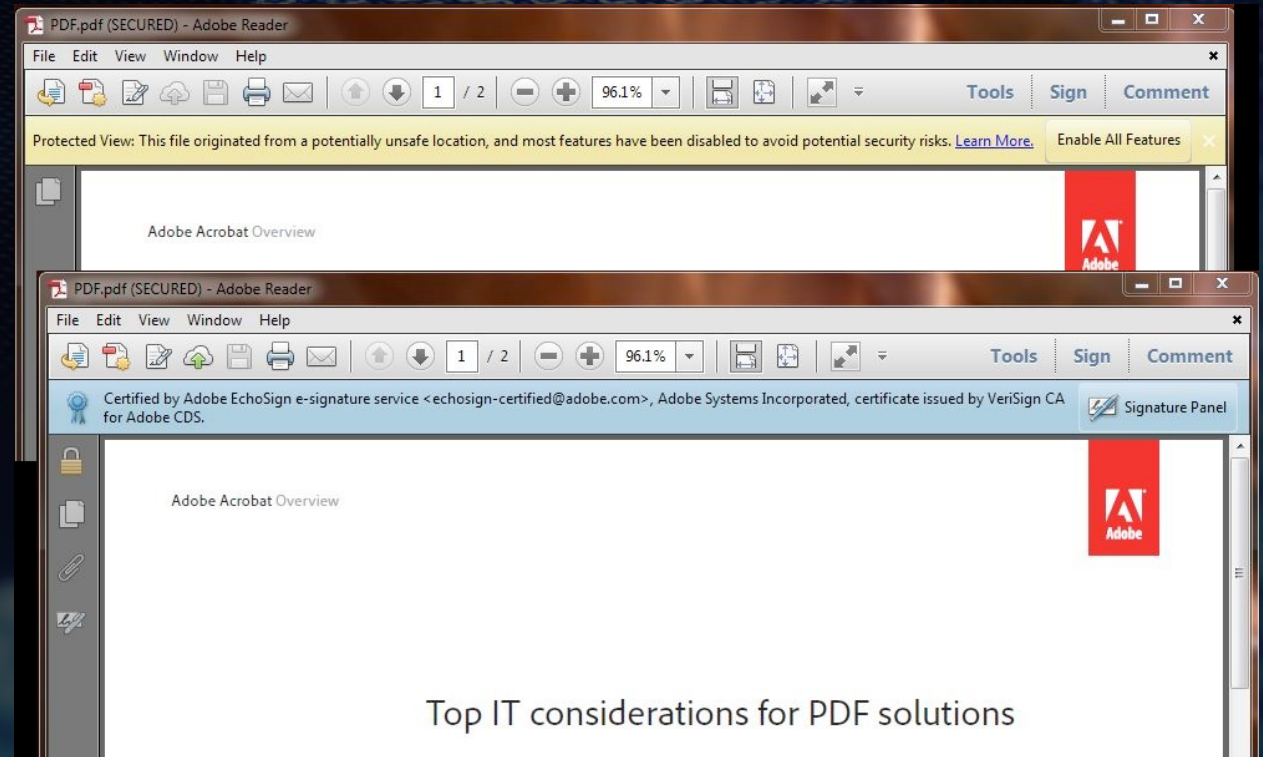
- **Adobe Currently Supports**

- P256 with digest algorithm SHA256
- P384 with digest algorithm SHA384
- P521 with digest algorithm SHA512



Leveraging Digital Signatures for additional Security

- **Mobile Code**
 - Untrusted JavaScript
 - Digital Signature Validation Required to Run JavaScript
- **Application Security**
 - Sandboxes
 - Exiting with a Better Informed Decision



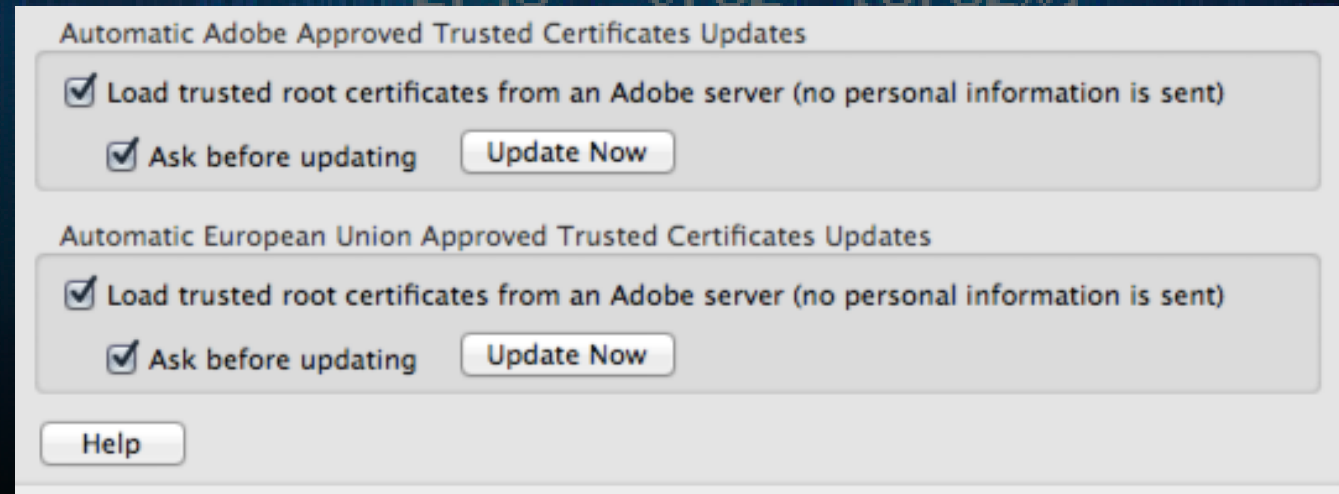
Extending Trust

- **AATL (Adobe Approved Trust List)**

- The Trust Dilemma
- Automating Trust

- **EUTL (European Union Trust List)**

- ETSI (European Telecommunications Standards Institute)
- Currently in Beta



A Few Parting Thoughts... And, Questions?

✓ Questions?