# Adobe Digital Signatures and Elliptic Curve Cryptography

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

# 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

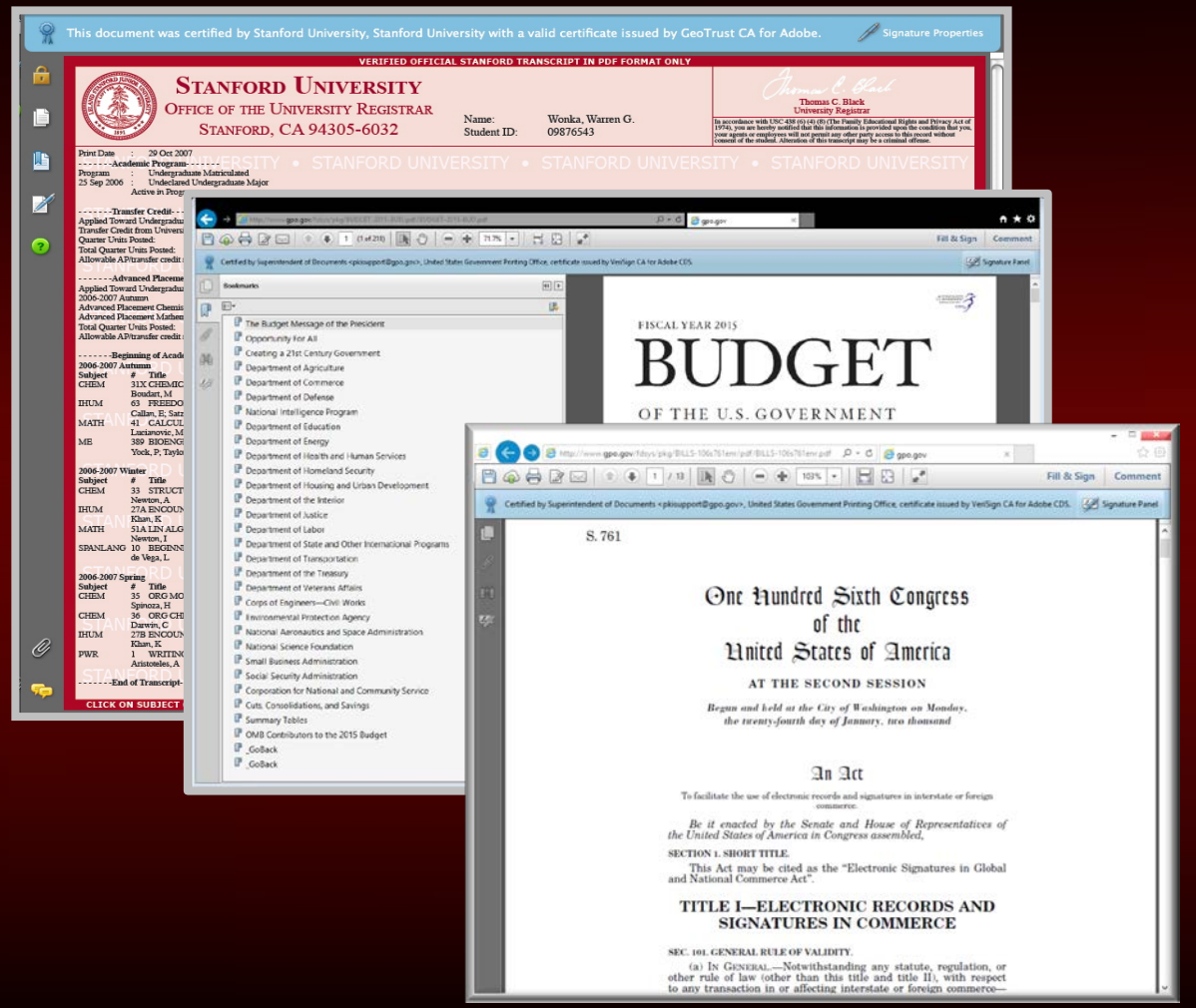


Adobe

# 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



# Elliptic Curve Cryptography

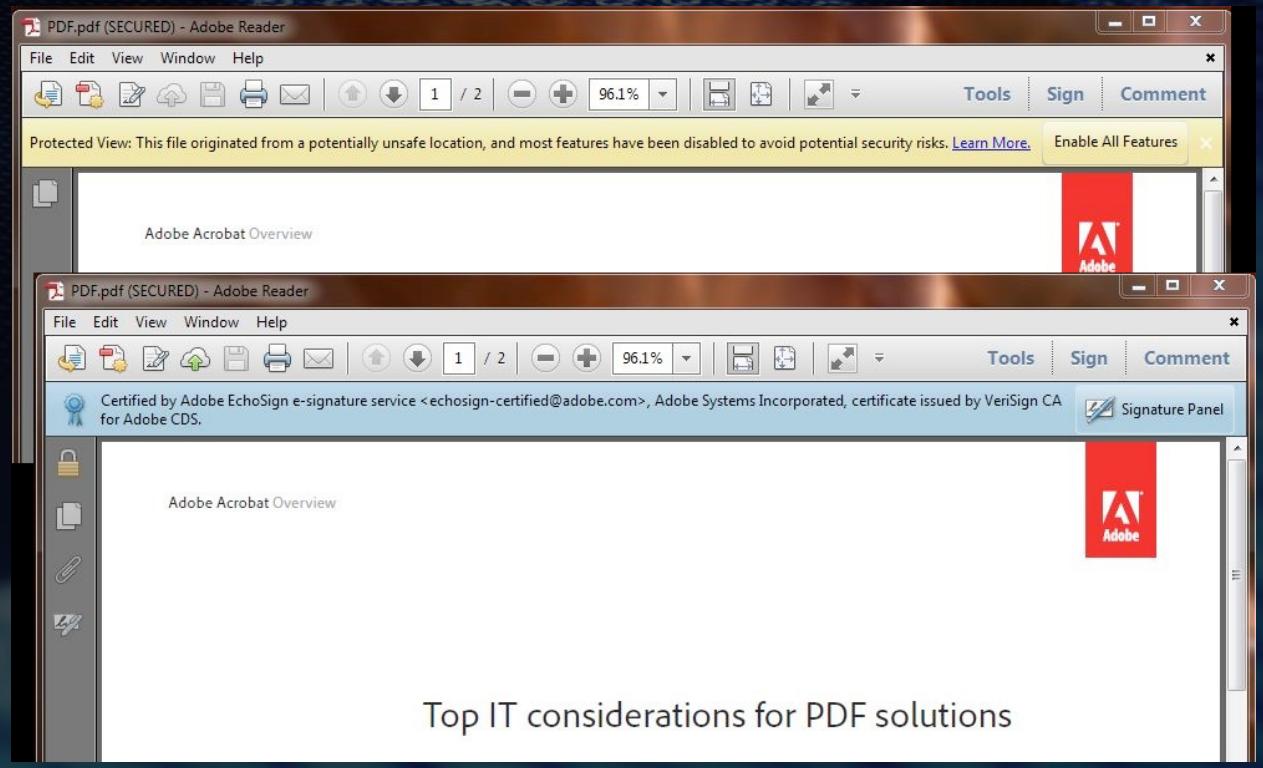
- **Digital Signatures**
  - One-Way Hash Function (Data to be Signed)
  - Public Key Cryptography (Hash)
  - Historically RSA, DSA
  - ECDSA has Emerged!
- **Adobe Currently Supports**
  - P256 with digest algorithm SHA256
  - P384 with digest algorithm SHA384
  - P521 with digest algorithm SHA512



Adobe

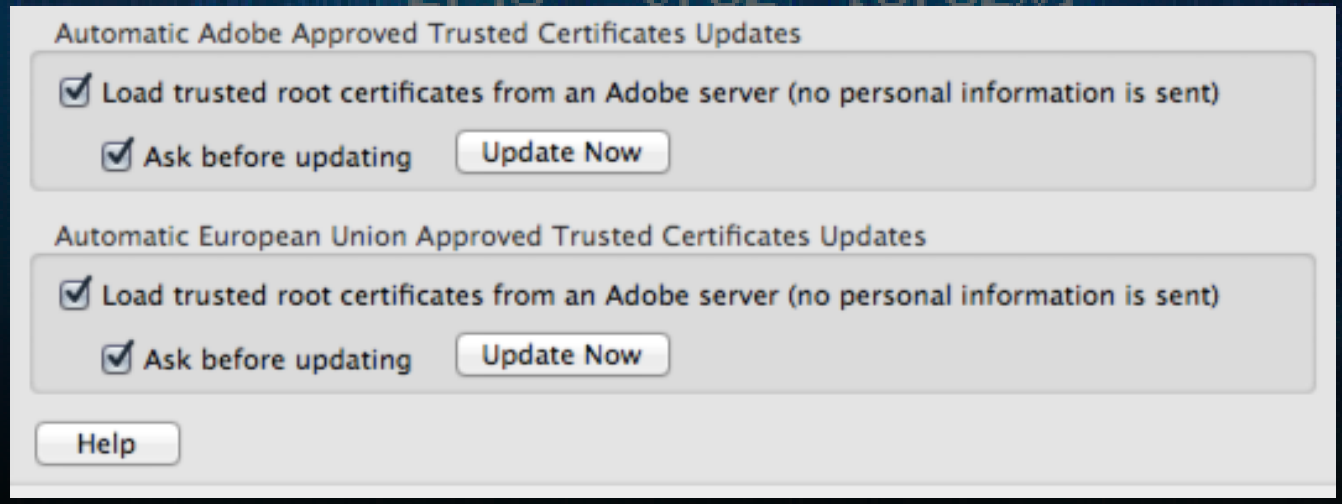
# Leveraging Digital Signatures for additional Security

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



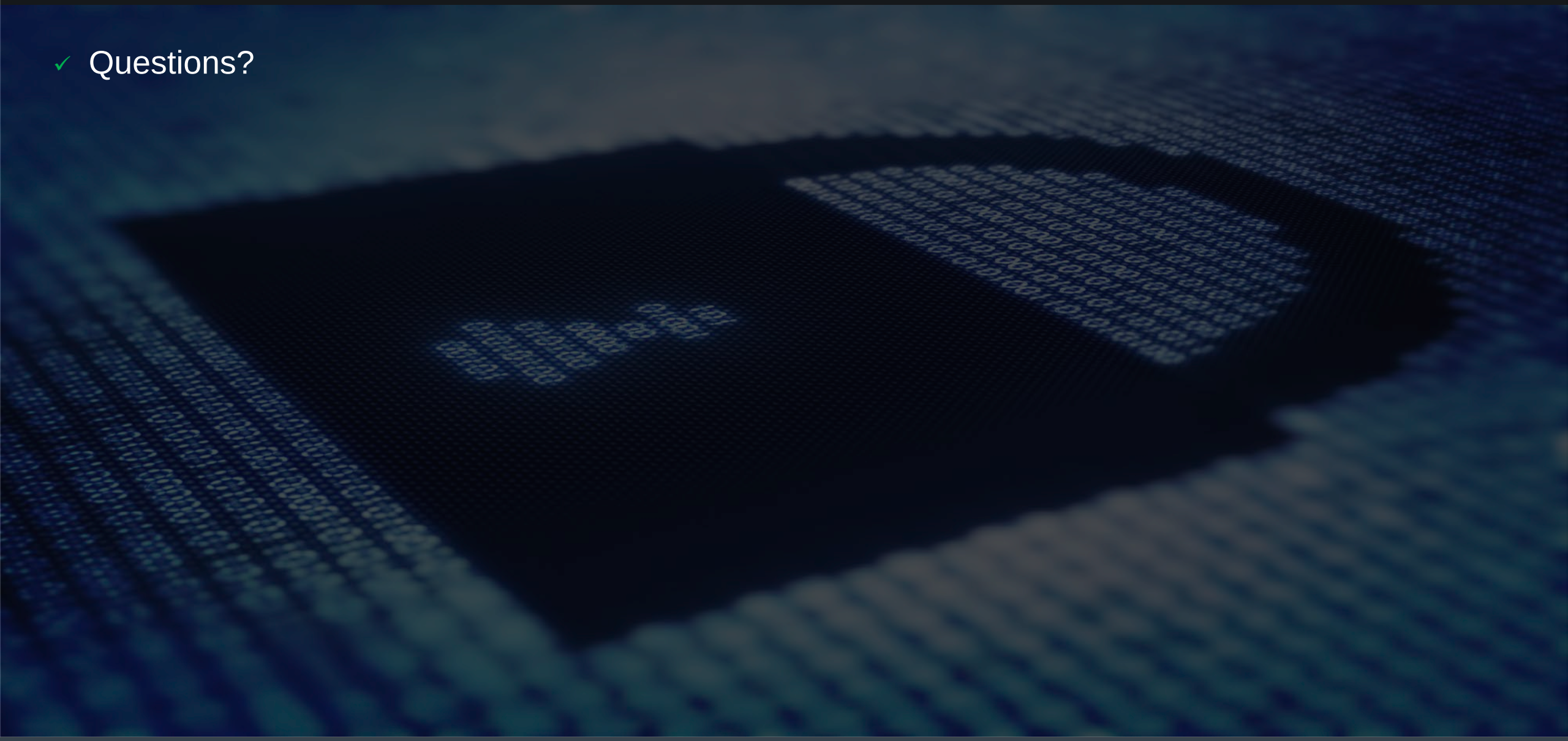
# Extending Trust

- **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?





Adobe