Security & Privacy at the IRS

September 19, 2002

Len Baptiste

SECURITY SERVICES

- Balance user and security needs.
- Work with MITS and Business to better define security roles and responsibilities.
- Three executive-led security offices.

SECURITY POLICY SUPPORT & OVERSIGHT

- Focus on 15 security capability areas in the Treasury/IRS Security Assessment Framework.
- Direct support to security policy governance processes.
- Lead on post 9/11 physical and operational security initiatives.

MISSION ASSURANCE

- Enhanced security incident response capabilities.
- Emergency preparedness capabilities.
- New certification and accreditation strategies.

MODERNIZATION SECURITY

- Oversight of PRIME security activities.
- Direct support to BSMO in oversight and acceptance of ELC security deliverables.
- Ensures adequacy of security architecture and engineering in integration of modernized and installed systems base.

PRIVACY ADVOCATE'S OFFICE

- Ensures that IRS policies and programs incorporate taxpayer and employee privacy concerns.
- Enable business owners and system developers to identify and evaluate privacy risk through the Privacy Impact Assessment tool.
- Communicate privacy objectives to the public and their representatives.

DISCLOSURE OFFICE

- Reviews systems under certification for compliance with the Privacy Act and IRS confidentiality requirements (UNAX).
- Makes determinations on whether a new Federal Register system of records notice is required.

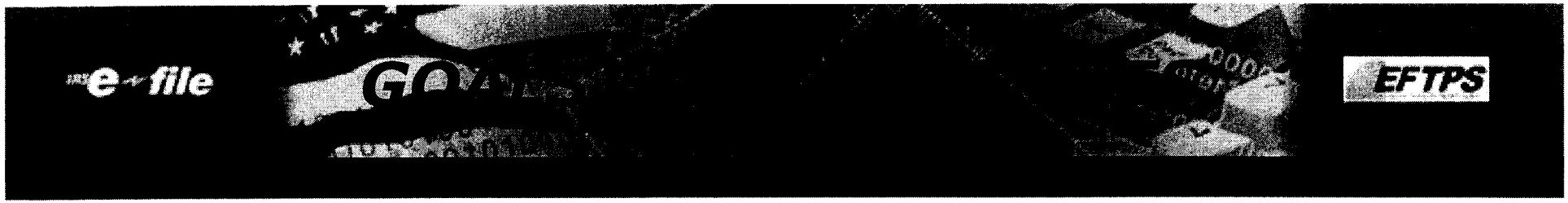
SAFEGUARDS OFFICE

- Provides security guidelines, IRS PUB 1075, to agencies and outside contractors that process, store, or transmit federal tax information under the provisions of Internal Revenue Code Section 6103.
- Provides onsite reviews of recipient facilities for compliance with safeguard requirements.

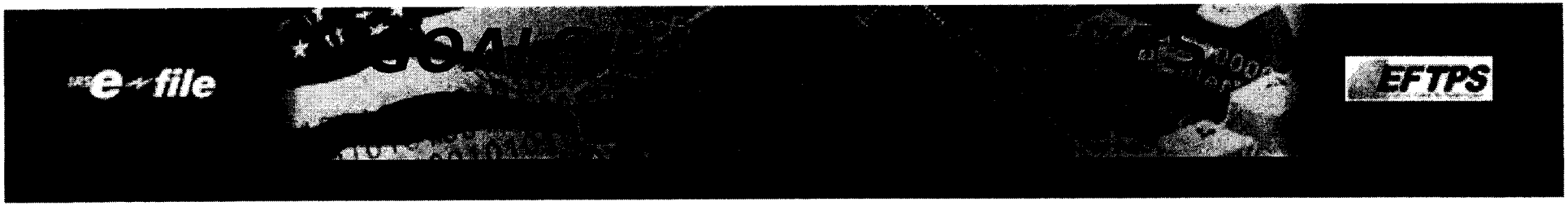
SECURITY AND PRIVACY AT THE IRS

Terence H. Lutes

September 19, 2002

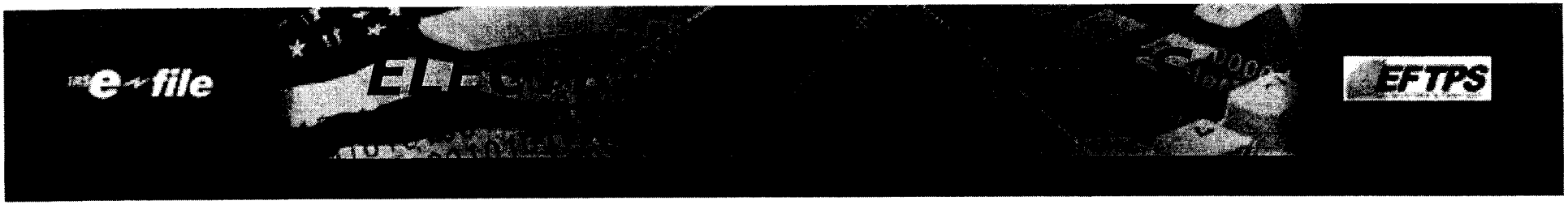


- The IRS Restructuring and Reform Act of 1998 (RRA98) is a major force behind IRS e-file
  - It requires that 80% of all Federal tax and information returns be filed electronically by 2007
  - Electronic account access by 2007, if secure
  - This sets the IRS GPEA-equivalent goal



- Although IRS is exempt from GPEA, efforts are very much the same
  - Plans for accepting forms, schedules and other information collection instruments electronically
  - Plans to accept electronic signatures
  - GPEA reports to OMB

Individual Taxpayers:	2001	9/12/02
Practitioner	28,929,694	33,175,715
On-Line	6,825,036	9,407,970
TeleFile	4,419,449	4,176,464
Total	40,174,179	46,760,149
4868 (Extensions)	312,534	636,215
Fed/State	15,210,640	19,207,894
Credit Card	296,996	275,377
Direct Debit	455,044	363,448
IRS.Gov Hits (Billions)	2.53	3.05



Business Taxpayers:	2001	2002
940	748,465	764,538
941 *	4,090,402	4,832,470
1041	1,445,223	1,559,365
1065	7,735	20,963
1065 (K-1s)		2,178,794
1120		Being Developed
EFTPS (FY)	60,860,453	58,258,853
FIRE	327,496,987	375,400,705

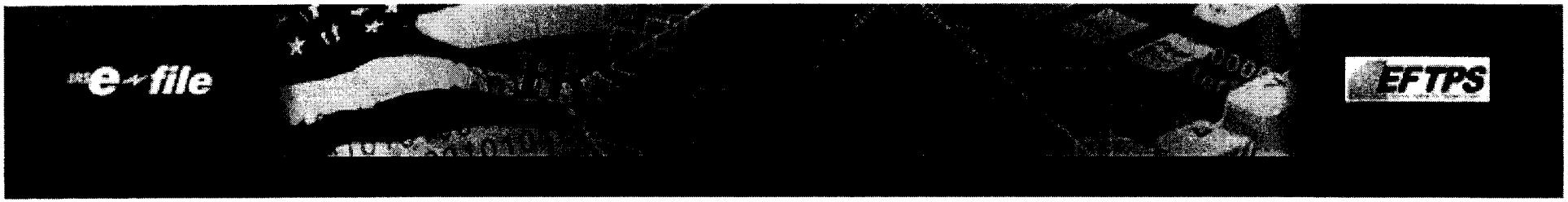
* (2nd Qtr 2001, 4-1 to 6-30)

- E-Services
  - Registration/application
  - PTIN application
  - Indirect channel management
  - Transcript delivery
  - Electronic account resolution
  - TIN matching

- Modernized E-File

- E-Government
  - EZTax
  - Expanding Tax Products for Businesses
    - Business returns (1120, 94x, 8850)
    - Online EIN
    - Harmonized Wage Reporting, SPEF, Standardized EIN

- Cost and Complexity
  - Practitioner, On-line (consumer)
  - Software and transmission (practitioner/software co.)
- Technical Infrastructure
  - 1960's legacy, 1985 e-file design
- Taxpayer Adoption
  - Individual/business
  - Marketing challenge
- Security and Privacy
  - Taxpayer concerns same as consumer concerns
  - Concern about third parties
  - Good messages but hard to deliver



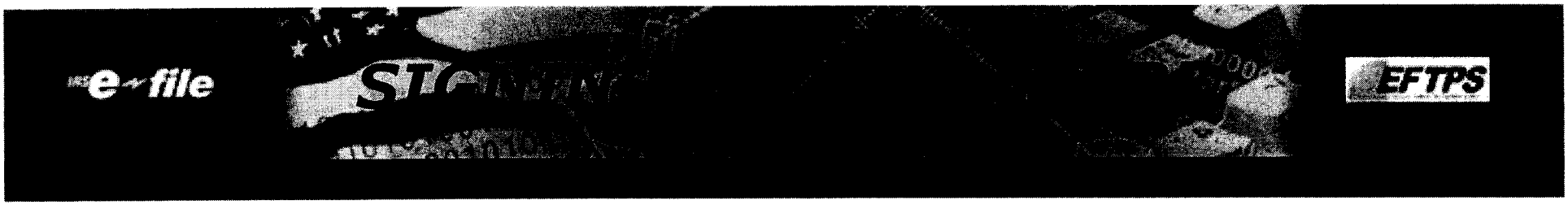
- Authentication: a security measure designed to establish the **validity** of a person, system, transmission, etc.

- Signature: an act undertaken by an individual to indicate the person's **identity**.

- Establishes the identify of a person or subject

- Requires registration with, and validation by, a third party

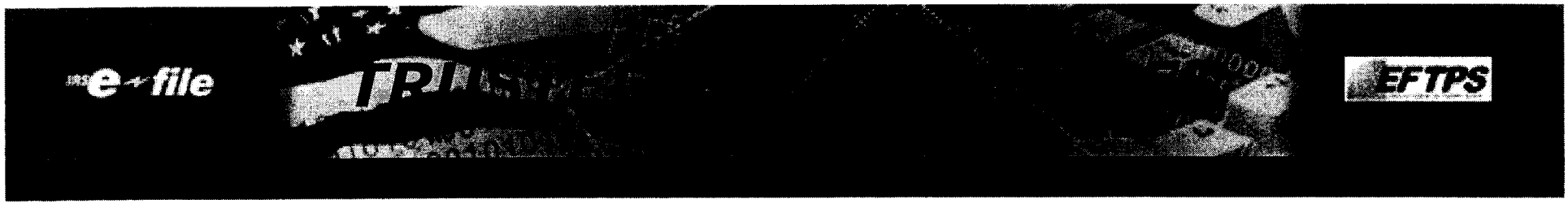
- Is used at the <u>beginning</u> of a transaction before rights or privileges are granted



- Binds together: the contents of the signed object, the signer's identity and the signer's intention to accept

- Does not usually require prior registration or enrollment

- Used <u>after</u> a transaction to determine accountability in the event of a dispute



- It's a Privilege to Participate - Not A Right

- Undertake a Stringent Application and Certification Process
  - Suitability Check Process
  - Participation Rules
  - Monitoring

- Individual E-File:
  - Approve the practitioner
  - Approve the software/transmitter
  - Authenticate the transmitter/software/ practitioner
  - Authenticate the Taxpayer/Signature
  - Accept the Return

- Business E-File:
  - Approve the software/transmitter
  - Approve the Practitioner
  - ***Determine Company Signature Authority***
  - Authenticate the transmitter/software/ practitioner
  - Authenticate the Taxpayer/Signature
  - Accept the Return

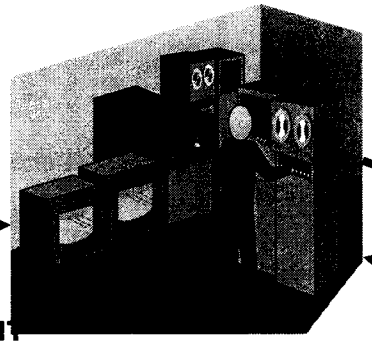
THE IRS e-file PROCESS

ON-LINE FROM HOME

TRANSMISSION

AUTHORIZED IRS *e-file* PROVIDER

ACKNOWLEDGMENT

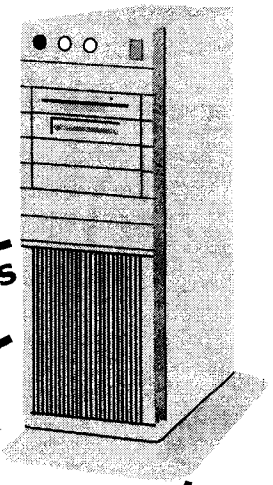


ELECTRONIC MANAGEMENT SYSTEM EMS

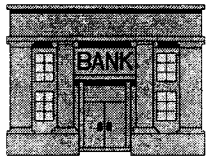
DRAINED FILES

ACKNOWLEDGMENTS

UNISYS

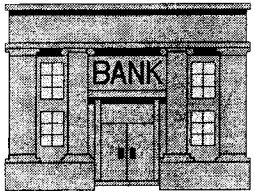


DIRECT DEBITS

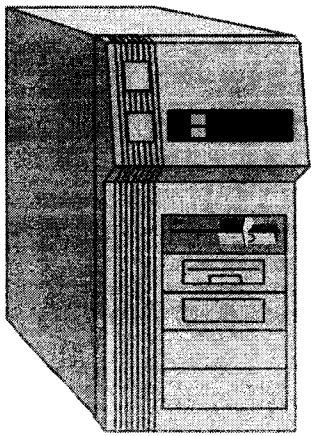


FINANCIAL AGENT

GOOD TAPE

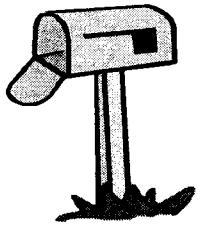


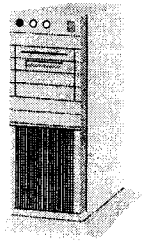
REFUND DIRECT DEPOSITED



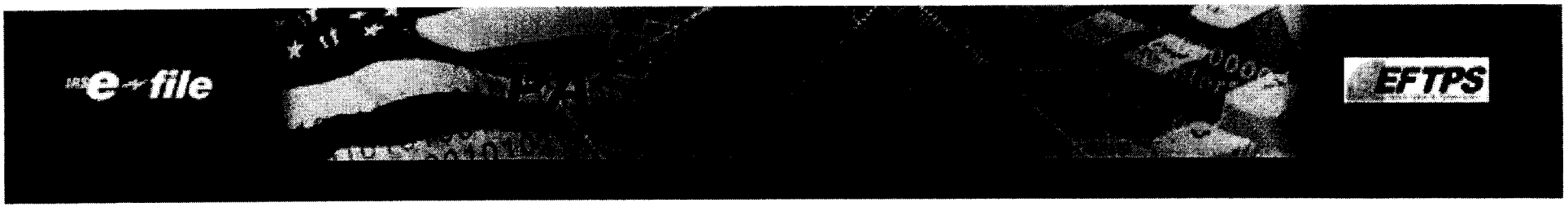
MCC

REFUND MAILED

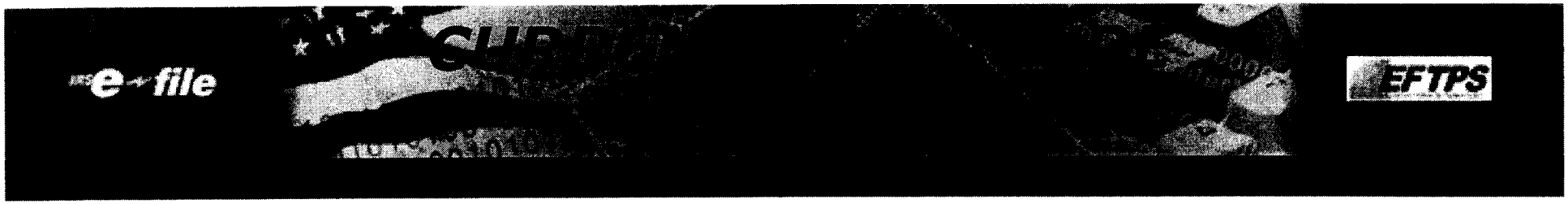




TRDB

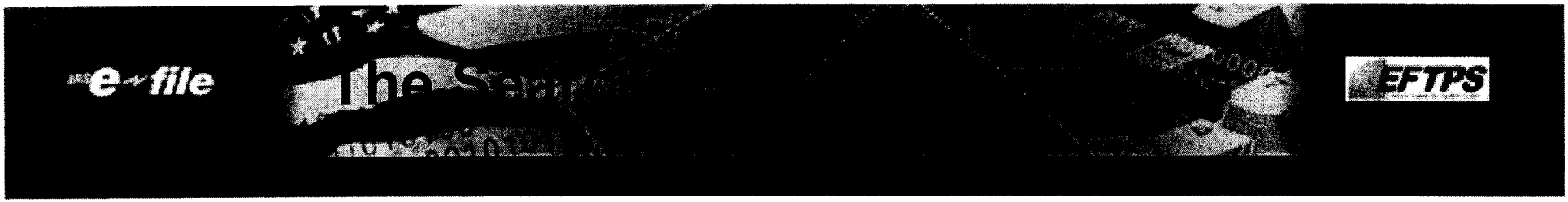


- What We Have Tried:
  - Digitized Signatures Pad
  - IRS generated Personal Identification Number (PIN)
  - PKI with Practitioners

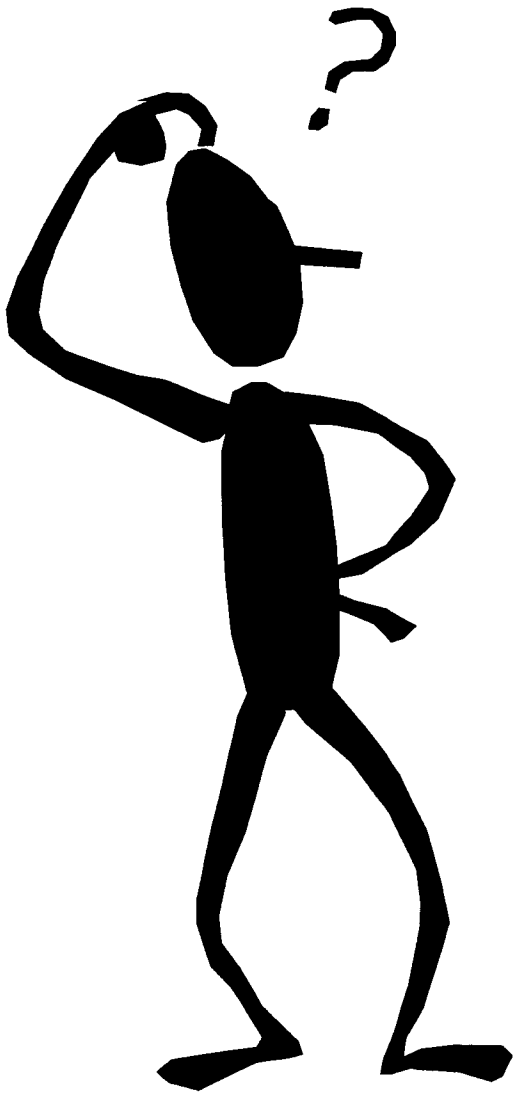


- What We Are Using Today For Individual E-File:
  - Form 8453
  - Practitioner PIN
  - Self-Select PIN

- What We Are Using Today for Business E-File:
  - PIN issued by CDB (94X only) (Terry -- we validate according to the EIN)
  - Form 8453



- Alternatives being discussed:
  - Voice signatures
  - PKI in certain instances
  - Credit/debit smart cards



Are any of these what I expect in an electronic transaction?

- Electronic signature needs to be as easy as signing a paper return.

- For the taxpayer authentication/signature on a tax return should be no more complex than making a purchase from a commercial web site.

- Use of Data by a Third Party

  - Section 7216 requires taxpayer consent in each case to use data stored by the practitioner/preparer.

  - Anything not covered by Section 7216 is covered under the Gramm Leach Bliley Act (Public Law 106-102)

- Basic processing the same as current on-line e-file

- Are requiring third-party privacy/security certifications
  - Challenge is identifying acceptable certifiers
  - Security certification of particular concern due to potential cost for small companies