15 April 2004

Ms. Marlene H. Dortch
Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W. Room TW-A325
Washington DC 20554

Re: ***Ex Parte* Presentation**
In the Matter of United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, RM-10865

Dear Ms. Dortch:

This is to inform you that Anthony M. Rutkowski of VeriSign, Inc., met on 14 April 2004 with: Ed Thomas, Chief of the Office of Engineering & Technology; Julius Knapp, OET Deputy Chief; Jeff Goldthorp, OET Chief of the Network Technology Division; Geraldine Matise, Deputy Chief of the OET Policy & Rules Division; and OET staff, Behzad Ghaffari, Rod Small, Jim Schlichting, and Jerry Stanshine; Cathy Zima, Acting Deputy Chief of the Wireline Competition Bureau Industry Analysis and Technology Division; and WCB staff Dave Ward and Mike Goldstein; and Media Bureau staff Alison Greenwald and Kyle Dixon.

The purpose of this meeting was to provide information regarding CALEA for VoIP and IP-Enabled Services: Industry solutions underway for meeting global mandates. The associated slide presentation by the same name is a faithful and complete representation of what was discussed.

VeriSign is a globally recognized leader in providing an array of large-scale, ultra-high availability infrastructure support capabilities for Internet, traditional voice telecommunications, security, and financial transaction services to providers and consumers through its various divisions in the U.S. and worldwide. As part of these commercial infrastructure support services, it provides lawfully authorized electronic surveillance (lawful interception) capability requirements to communication providers globally, other lawful access services (i.e., subpoena processing) and participates in or leads many of the related technology, industry, and standards activities. VeriSign also collaborates closely with industry product vendors worldwide, and looks forward to assisting the Commission in considering matters relating to the subject rulemaking proceeding.

Pursuant to the Commission's rules, this *ex parte* letter together with the slides will be filed via the Commission's Electronic Comment Filing System for inclusion in the public record of the above-referenced proceeding.

Respectfully submitted,

/s/

Anthony M. Rutkowski
Vice President for Regulatory Affairs
VeriSign Communications Services Div.
21355 Ridgetop Circle
Dulles VA 20166-6503
tel: +1 703.948.4305
mailto:trutkowski@verisign.com

cc: Ed Thomas
Julius Knapp
Jeff Goldthorp
Geraldine Matise
Behzad Ghaffari
Rod Small
Jim Schlichting
Jerry Stanshine

Cathy Zima
Dave Ward
Mike Goldstein

Alison Greenwald
Kyle Dixon

Federal Communications Commission
Washington DC
14 April 2004

CALEA for VoIP and IP-Enabled Services: Industry solutions underway for global mandates

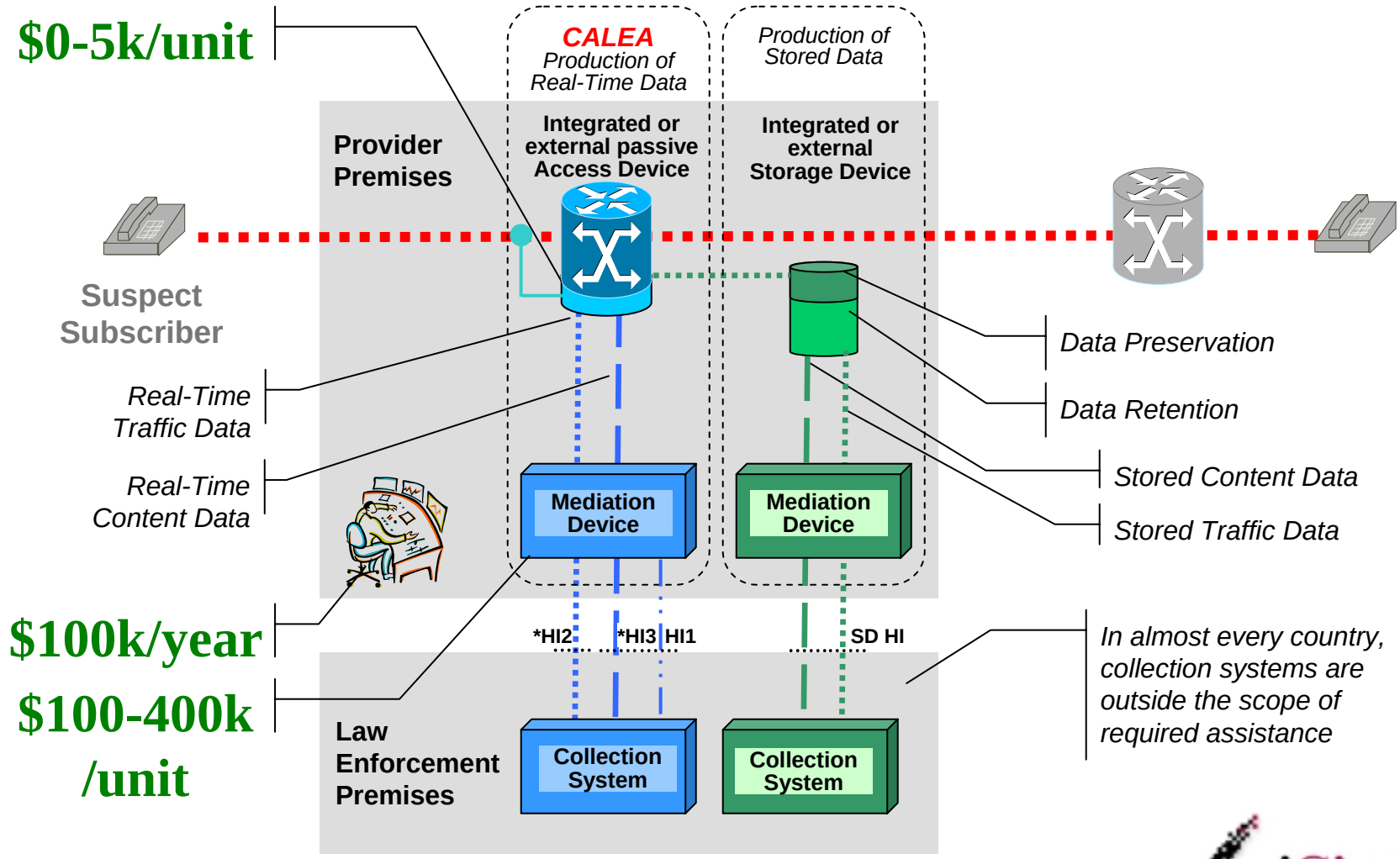
Anthony M. Rutkowski
VP for Regulatory Affairs
VeriSign, Inc
Dulles VA
mailto:trutkowski@verisign.com

Principal Points

- **A global industry constellation of vendors, platforms, and forums are effectively addressing LI/LAES forensic capabilities for VoIP and IP-enabled services**
  - Responsive to common law enforcement forensic needs, national regulatory mandates, fraud management and network protection needs worldwide
  - Necessary implementations for Law Enforcement will not occur absent regulatory mandates that should include regular compliance testing
  - U.S. law enforcement – even with Joint Petition capabilities – has considerably less than in most nations - adversely affecting U.S. national security
  - Standards, equipment, cost-effective service bureau solutions exist already
  - No observed or plausible adverse effects on technologies
  - Architectures dramatically affect costs
- **Time to eliminate Packet-Mode, Circuit-Mode fiction**
- **Forensic challenges for industry today**
  - Fewer, interoperable, global VoIP and IP-Enabled Service standards and identifiers
  - Distributed networks and applications
  - Transnational capability implementations
  - Small local access providers – particularly those providing public access promiscuously
  - Subscriber identification and subpoena costs
  - Enhancing accuracy, authentication, accountability
- **Transition to service bureaus to meet the challenges**

VeriSign®

Forensic capabilities for VoIP and IP-enabled services



*referred to as “e” interface by most U.S. standards bodies

Architecture dramatically affects costs

On the customer premises, Service Bureau can provide:

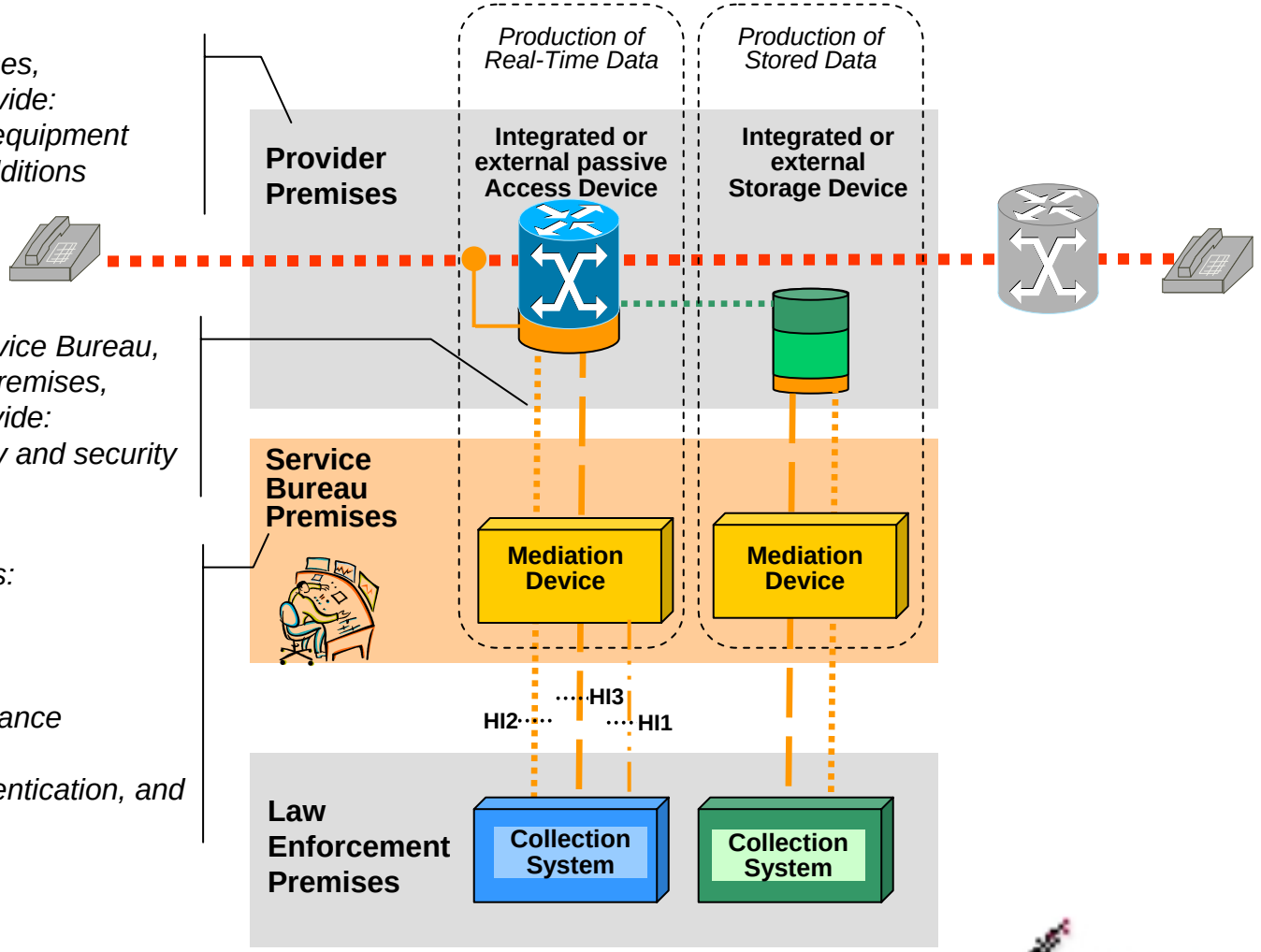
- *Necessary network equipment modifications and additions*

Between Customer, Service Bureau, and Law Enforcement Premises, Service Bureau can provide:

- *Required connectivity and security*

Service Bureau provides:

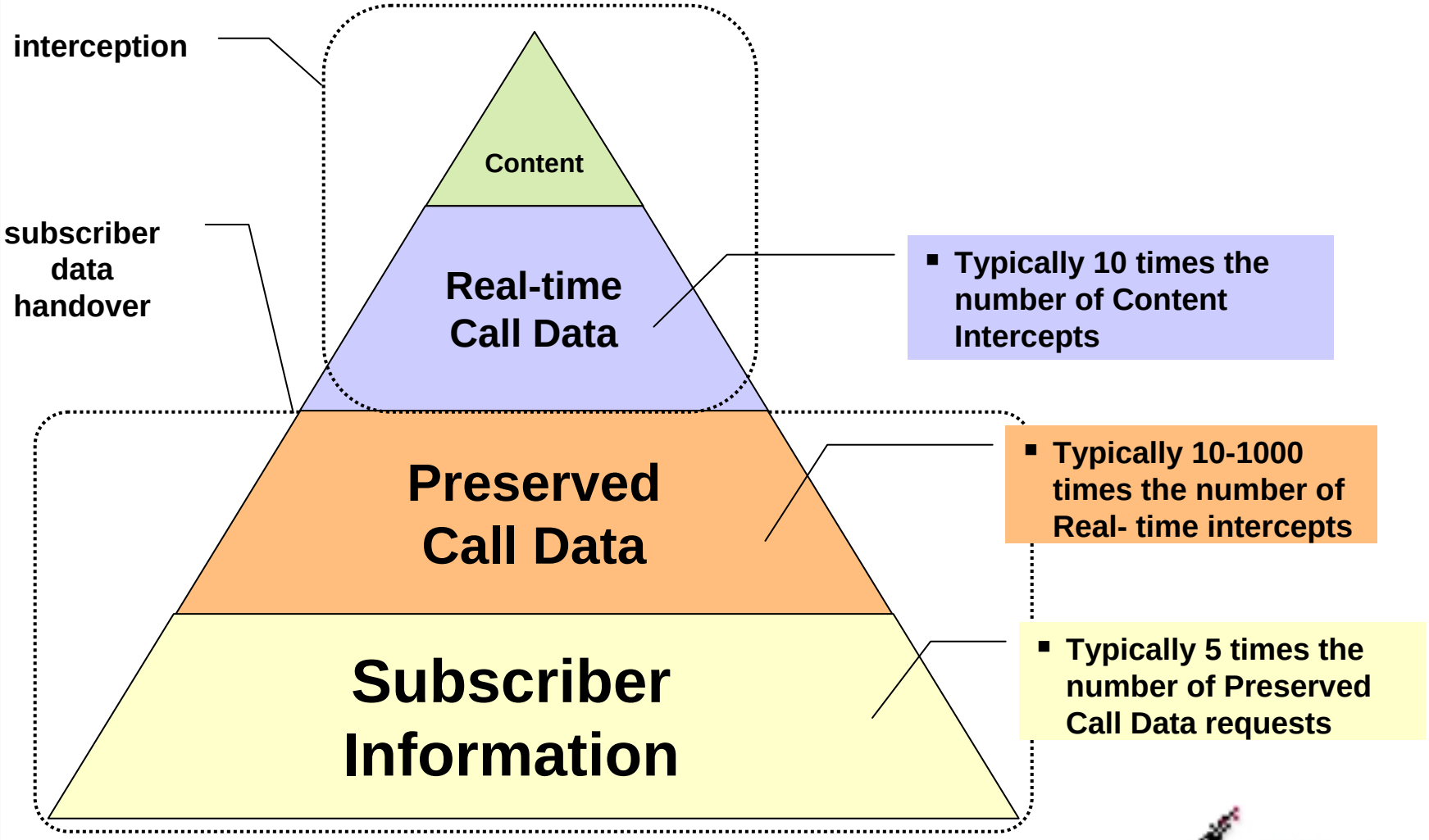
- *Mediation Devices*
- *Security Office*
- *7x24 Support*
- *Testing and maintenance*
- *Capability upgrades*
- *Administration, authentication, and accounting*



This diagram depicts VeriSign's NetDiscovery service bureau.
Not all service bureaus may offer these capabilities.

VeriSign®

Handover Data Pyramid



VeriSign®

Global LI industry constellation: vendors, standards fora, law enforcement

Product Vendors

(access, mediation, collection, analysis)

Accuris	x	x	x	
Acecom			x	
ADC	x	x		
Aqsacom	x	x	x	
Bartec			x	
Cetacean			x	
Cisco	x			
Ericsson	x			
ETI	x	x	x	x
i2				x
JSI	x	x	x	
Juniper	x			
Lucent	x			
Marconi			x	
Motorola	x			
Narus	x			
Nice	x	x	x	
Nokia	x			

Nortel	x			
Orion				x
Pen-Link			x	x
Pine	x	x	x	
Raytheon			x	
Roke Manor			x	x
SAIC			x	x
Septier		x		
Siemens	x	x	x	x
Spectronic				x
SS8	x	x		
Syborg				x
SyTech				x
Thales				x
Top Layer	x			
Ultimaco	x	x	x	
Verint	x	x	x	x

Many also maintain proprietary standards

LI Standards Fora

ETSI	LI	Int'l
	3G	Int'l
	AT-D	Int'l
	TISPAN	Int'l
Cisco/IETF	LI	Int'l
CableLabs	PCESP	US
ATIS	T1S1	US
	T1P1	US
TIA	TR45.6	US
	TR45.LAES	US

Law Enforcement Agency Nations Shaping LI Standards

USA-FBI
Australia
Austria
Canada
Denmark
Finland
France
Germany
Italy
Netherlands
Russia
Spain
Switzerland
UK

Note: this list is based on visible participation, and is not represented as complete

Service Vendors

domestic, International, infrastructure

Fiducianet	x		
GTEN	x	x	
TSI	x		x
VeriSign	x	x	x

VeriSign®

Responsive to common needs worldwide

- **Law enforcement forensic needs**
  - Access to communications identifying information and/or content at the necessary network elements and handover to monitoring facility
  - Within required timeframes
    - Law enforcement effectively cannot do this except with the capabilities in place – the most fundamental purpose of CALEA
- **National regulatory mandates**
  - Almost every nation has CALEA-like requirements
  - Some impose significant stored data requirements
- **International treaty mandates**
  - Cybercrime Convention plus MLATs (Mutual Legal Assistance and other Agreements)
- **Fraud management and network protection needs worldwide**
  - Similar capabilities are being implemented by providers themselves to control fraud and protect network infrastructure

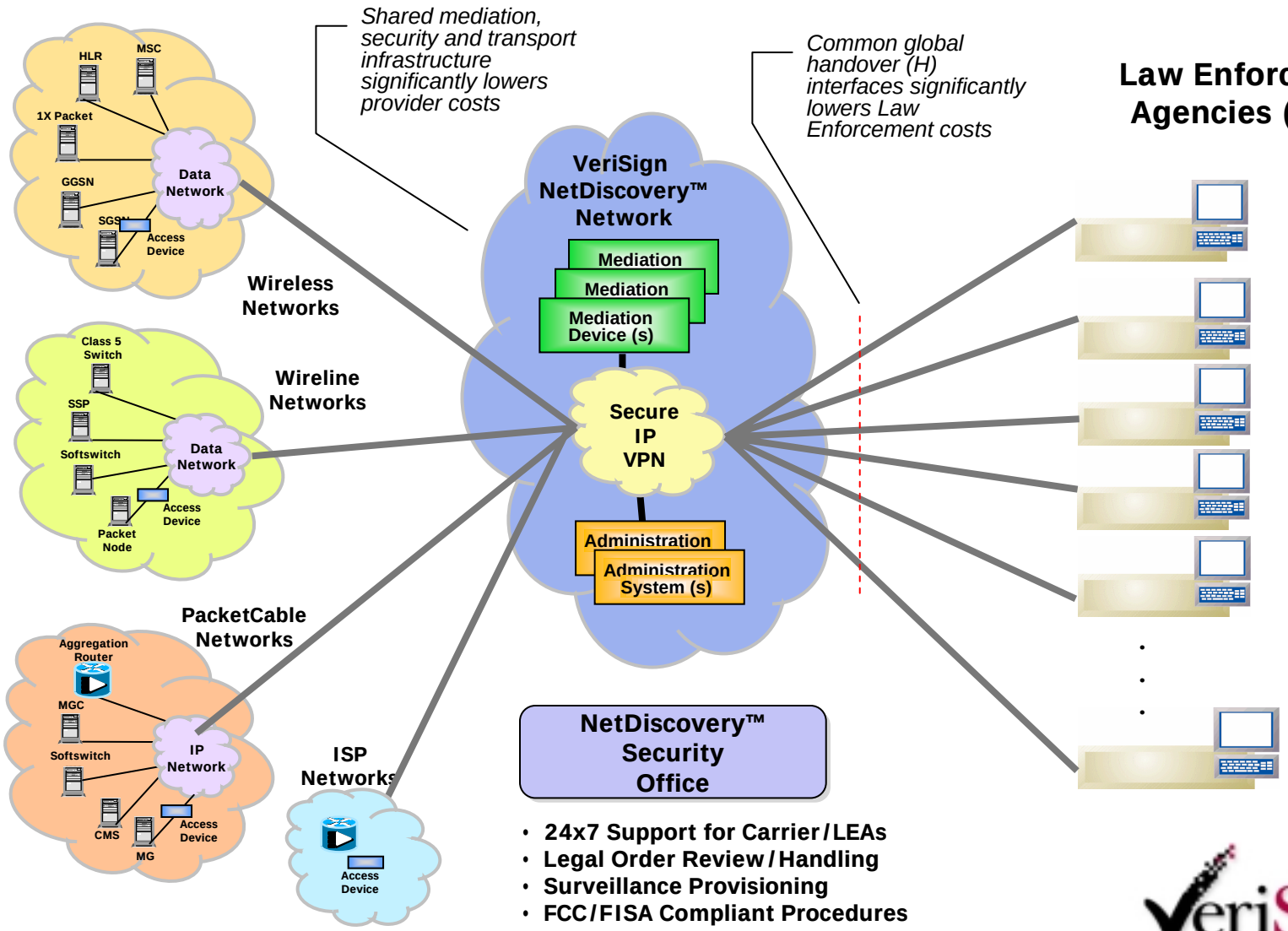
VeriSign®

Required LI capabilities for IP-Enabled Services exist today

- **LI industry driven by long-standing global marketplace for capabilities**
- **Standards**
  - Vertical LI market vendors began developing proprietary standards for law enforcement in the early1990s
  - Good collaborative industry LI standards forums emerged in Europe in the mid-90s
  - Initial IP national standards pioneered in The Netherlands circa 2000 and implemented by regional vendors
  - CableLabs pioneered work in the U.S. in 2001
  - Cisco mounted large-scale standards development effort innovatively based on SNMP and leveraging CableLabs and ETSI specifications; Juniper has an OS-based XML solution. Both are published in IETF specifications
  - ETSI began large-scale, comprehensive, international IP-Enabled Services standards initiative two years ago, and basic standards suite is complete
  - All other needed specification development efforts completed
    - ETSI 3G completed 33.108 specification
    - TIA TR45.6 completed CDMA2000 specification
    - ATIS completed wireline VoIP (T1.678) and UMTS (T1.724) specifications
- **Equipment and Software**
  - High performance, reliable systems based on proprietary systems have been around since early 1990s
  - Systems vendors today support a mix of proprietary, CableLabs, ETSI, and Cisco standards
- **Cost-effective service bureau solutions**
  - Most service bureaus – especially VeriSign – has solutions that are tested and implemented for provider customers today
- **No adverse effects on technology**
  - Implementation is an engineering issue, adverse effects are not encountered in practice, nor likely
  - Not relevant because the capabilities are required in almost every other country, and for network integrity purposes

VeriSign®

VeriSign's Service Bureau architecture



Regulatory mandates are necessary

- **All providers are highly unlikely to undertake to implement the necessary capabilities**
  - LI capability implementations to support law enforcement are a highly specialized activity not part of the provider's normal service provisioning
  - Requires end-to-end regular maintenance and testing
- **Even with regulatory mandates and severe penalties, many will take the risk**
- **Existing regulations do not even go so far as requiring implementation testing – ideally by a third party**
  - Commission required this for years by radio station frequency measurements
- **Telling law enforcement that they can come in and engineer the capabilities as needed in an investigation, and provide their own equipment, is not a solution**

VeriSign®

Strategic considerations

- **Most nations have more extensive LI requirements, many with technically advanced architectures and analytical systems – especially for mobile and IP-Enabled Services**
- **Most other nations require and obtain greater assistance to Law Enforcement by providers, well beyond Joint Petition capabilities**
  - Focus in most countries is on sophisticated analysis of retained data – which allowed post 9/11 tracking of terrorists in Europe
- **Almost all LI systems vendors are foreign based**
  - Diminishes U.S. R&D and knowledge base
  - Increases reliance on foreign vendors for systems development
  - Situation has become worse with Internet based services
- **Problems are exacerbated by failure to use international LI standards in the U.S.**
  - Common global handover standards significantly reduce costs for Law Enforcement and industry, as well as enhance capabilities
    - ETSI LI standards model emphasizes common base standard with national variants specified in annexes or national regulations
  - FBI has usefully shifted assets to international standards forums with support from industry
  - Provisions in Joint Petition would allow for greater use of international standards

VeriSign®

Packet-mode, circuit-mode fiction

- **In the real-world, almost all network communications have long been packet-based; "circuits" are created virtually**
- **The legacy 1980s telecom packet-circuit service distinction somehow became introduced into the U.S. CALEA debate for argumentative and tactical purposes**
- **Distinction has no basis in CALEA or Law Enforcement needs which are independent from transport protocols**
  - service capabilities-based and technology-neutral worldwide
- **All intercepts are accomplished by techniques that are irrelevant to variations in the transport protocol**
  - Passive replication and programmed extraction of desired signalling or content data in the transmission path
  - Directions to a network element (usually a switch/router), gateway device, or application server to detect and replicate a desired signal or content data
  - A software agent directed to detect and replicate desired signal, content, MIB, or log data
- **Fiction of a dichotomy**
  - Impedes meaningful industry collaborative activity
  - Use of consistent global interfaces and standards
  - FCC should immediately declare the fiction to be irrelevant – five years of "study" is enough

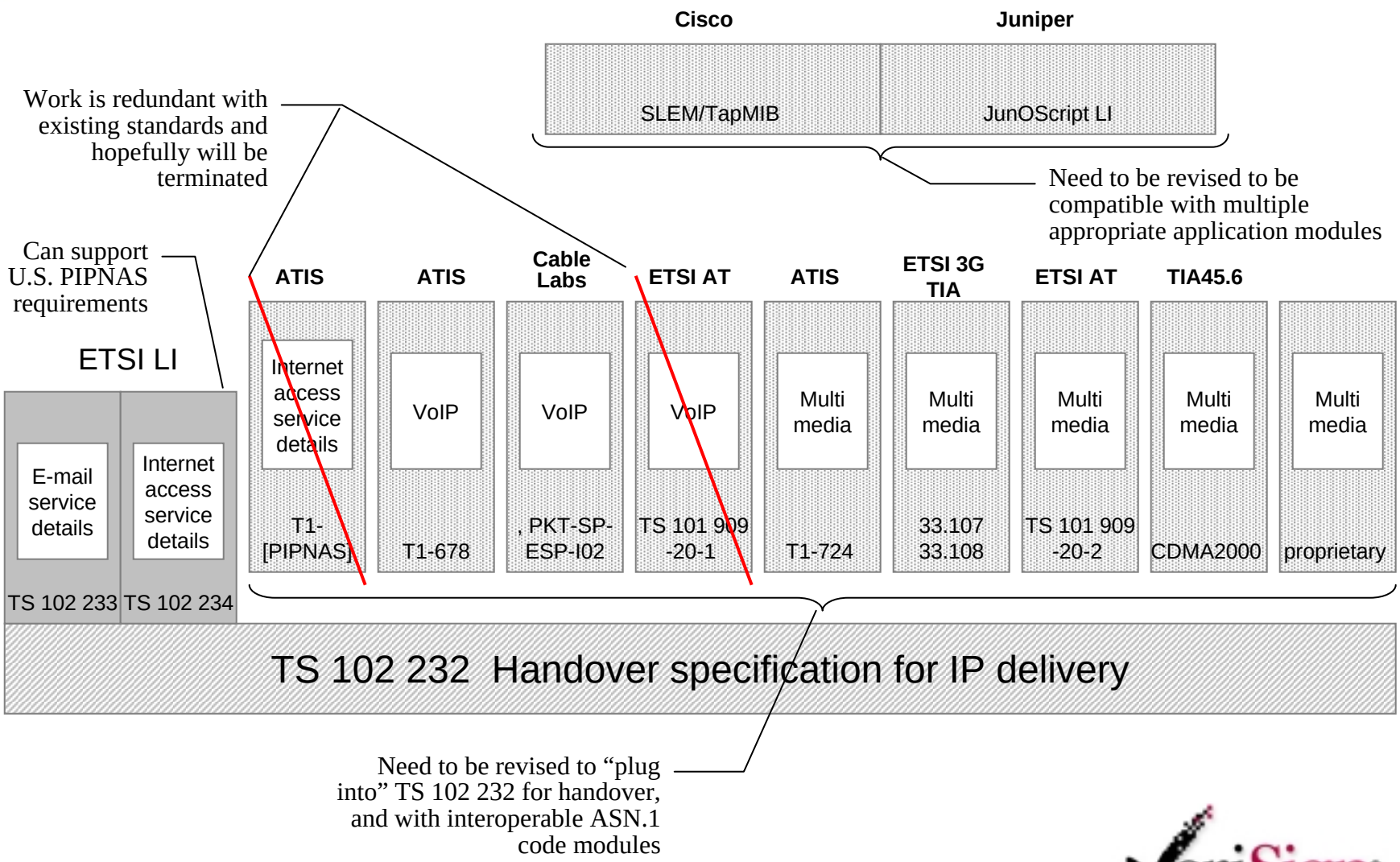
VeriSign®

Industry Challenges Today

- **Getting an effective CALEA mandate in place**
- **Converging on a common global model and standards**
  - Diminishes the pre-certification problem
  - Capabilities can be certificated by equipment vendors, if necessary through independent laboratories
    - VeriSign does this today
  - New collaborative activities planned for Asia-Pacific, Americas, Africa
- **Effective distributed LI capabilities, especially for**
  - Small-scale access providers
  - Promiscuous local access points
- **Transnational capability implementations**
  - Architectures and standards
  - Processes
- **Subscriber authentication and a common interface to stored data**
  - CALEA requires assistance in providing subscriber information
  - Costs are dramatically scaling

VeriSign®

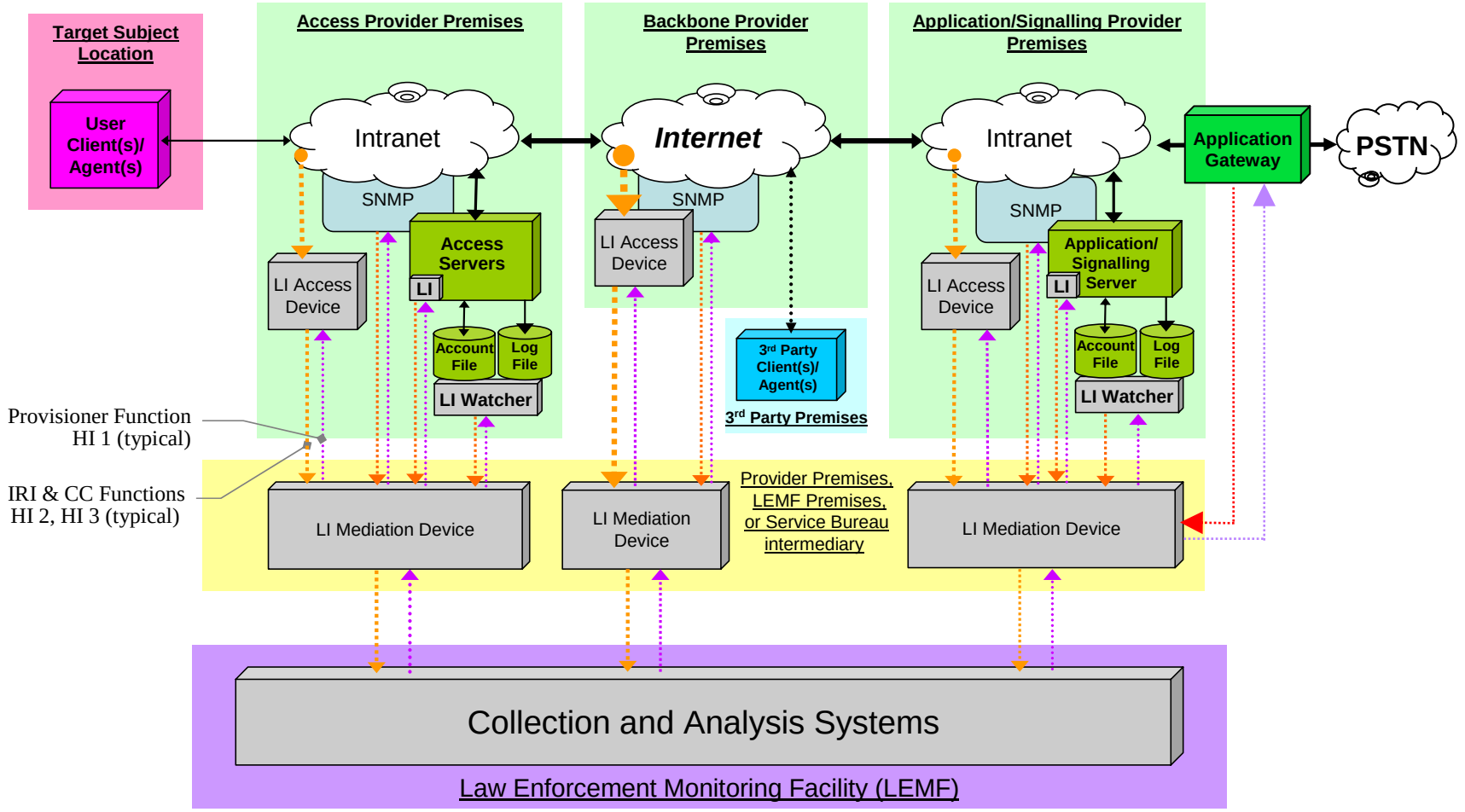
Converging on fewer, interoperable, global VoIP and IP-Enabled standards



Adopted as part of ETSI TC LI Future Workplan, Oxford UK, 23-25 Mar 2004

VeriSign®

The distributed network challenge

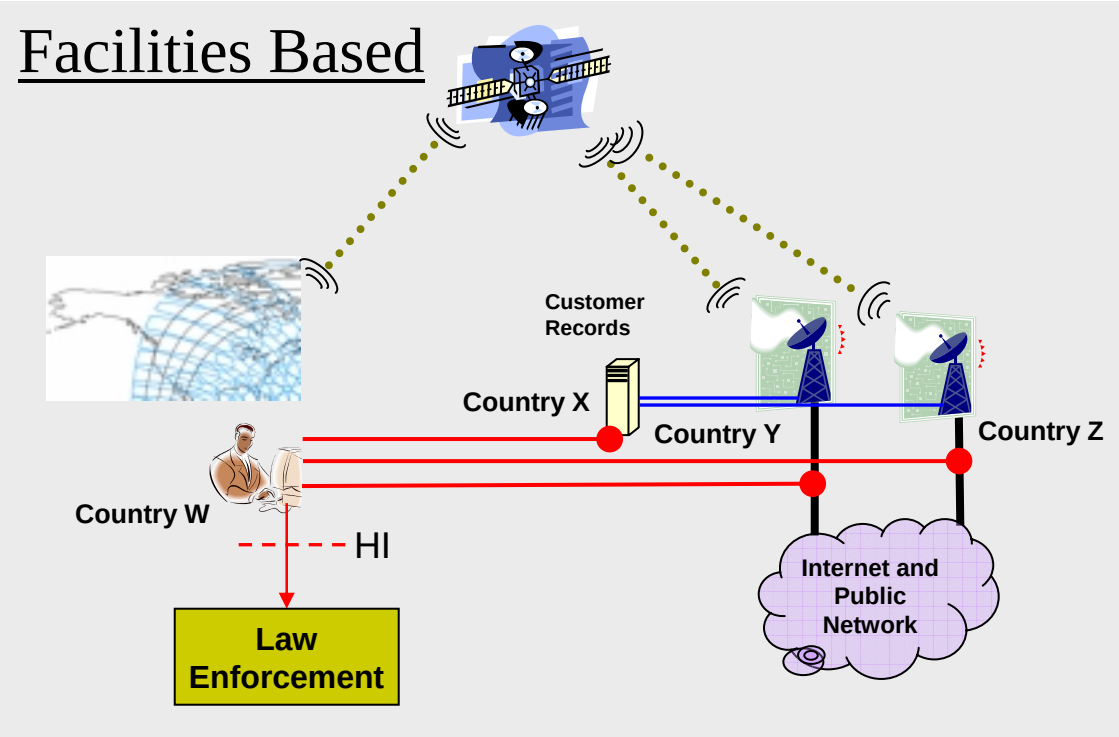


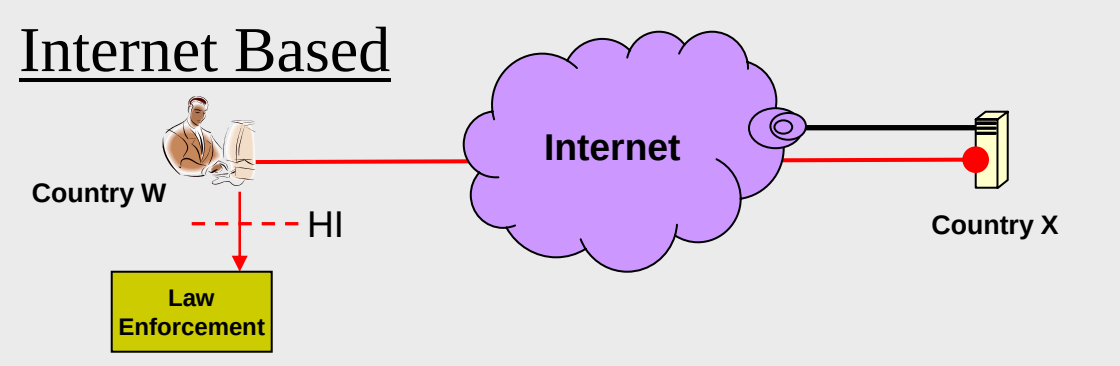
Common, deployed, global standardized interfaces are critical for required Law Enforcement capabilities and reducing costs

VeriSign®

The transnational CALEA challenge

Common, deployed, global standardized interfaces are critical for required Law Enforcement capabilities and reducing costs





VeriSign®

The small local access provider challenge

- **Applies to**
  - Hotels, rural carriers / ISPs, universities, cafés, airports, powerline providers, etc
- **May require special measures**
  - Flexible or special CALEA requirements
  - Alternative means of funding
- **Service bureaus offer effective solution to cost issues**
- **Entwined with subscriber identification challenge (next slide)**

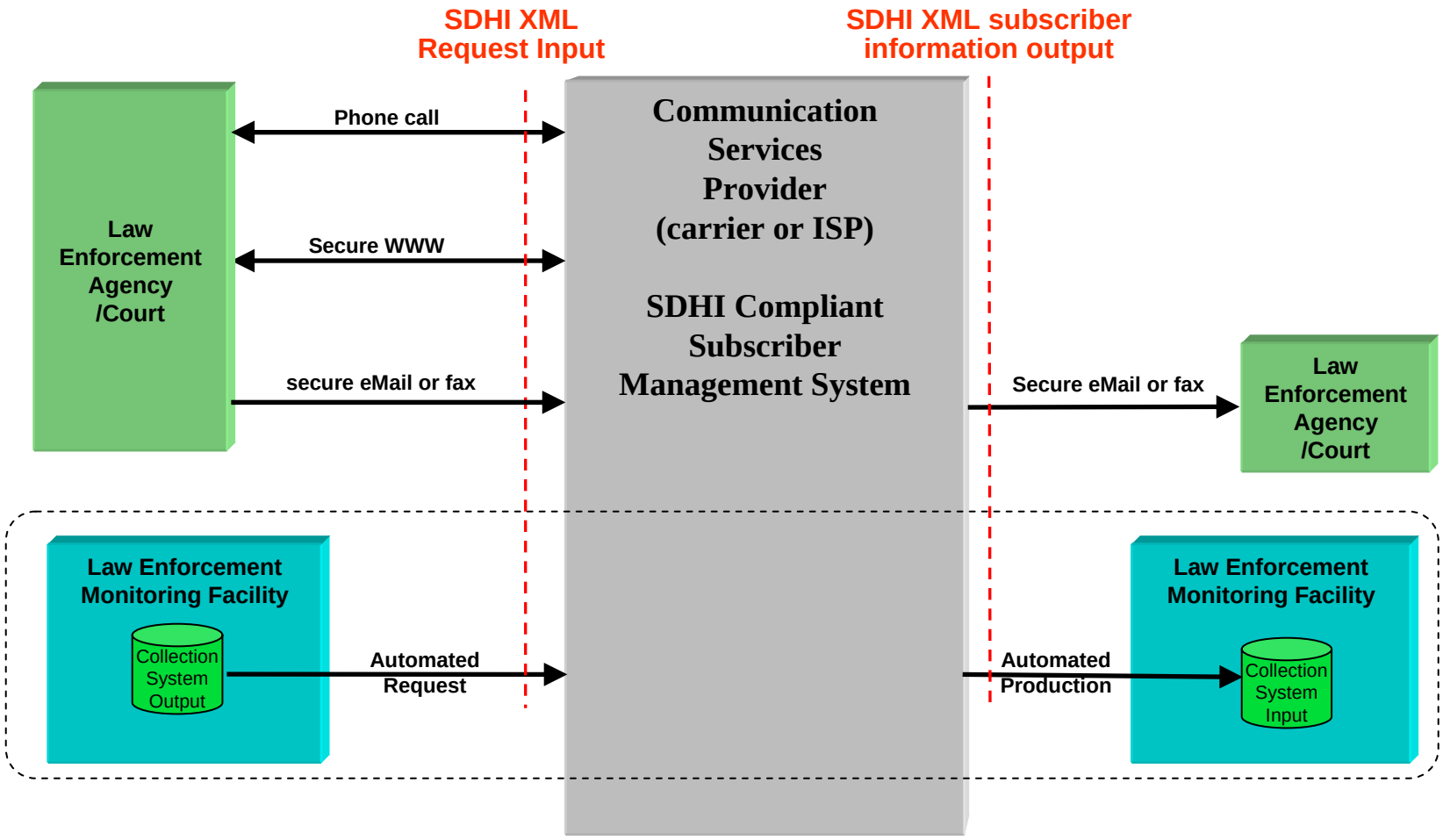
VeriSign®

The subscriber identification and subpoena costs challenges

- **Expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access available call-identifying information**
  - a fundamental Sec. 103 requirement of CALEA
  - a critical need worldwide
- **Generally was not problem in traditional telephony world**
  - Pre-paid cards, anonymous SIM cards, disposable cell phones began to change situation – now banned in some countries
- **Promiscuous, nomadic broadband access poses a significant challenge for law enforcement**
  - Capturing identity of accessing party is critical for fraud management and where required by Law Enforcement
- **May be ameliorated within industry itself by need to effect better business models, reduce fraud, protect network facility, and new object identification technology**
- **Common global standards being developed**
  - Internet Registry (IRIS) standard to for IP-Enabled Service providers – especially EREG for ENUM – which replaces old WHOIS standard. See http://www.ietf.org/html.charters/crisp-charter.html; http://www.verisignlabs.com/ (click on IRIS)
  - OASIS Subscriber Data Handover Interface (SDHI) for generic subscriber information See <http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=legalxml-sdhi>
  - Sec. 103 FCC regulatory mandate can include
  - Subscriber authentication requirement
  - Availability to Law Enforcement through standardized interface
  - Comports with Cybercrime Convention requirements

VeriSign®

A standard subpoena interface:
Subscriber data handover interface (SDHI)



Underway in global XML standards body – OASIS
Legal XML SDHI standards committee

VeriSign®

All previously described developments must address authentication, accuracy and accountability

- **Synergy among requirements**
  - Digital forensics
  - Privacy
  - Fraud management
- **Encompasses**
  - Parties to the processes
  - Instruments in the process
  - Data produced by the process
  - Chain of evidence
  - Record keeping and statistics
  - Post collection analysis
- **Involves**
  - Authentication of parties, instruments, network elements, and data
  - Integrity and security of the transport paths and data
  - Timing accuracies
- **Technology largely exists**
- **Standards being developed**
- **Related regulatory mandates receiving attention in UK and other countries**

VeriSign®