New Trade Landscape

Gene Panger

TUV Rheinland Group

Three Trade Characteristics Rising in Importance

1. Information Security Management Systems

2. Supply security

3. Authentication

Together: Security Assurance

1. Information Security Management Systems (ISMS)

- Formalize information security, provide harmonizing platform

- Enterprise-wide perspective

- Scope defined by organization and commercial agreements

- Focus: information assets, risk exposure, response

- Affects:

    - Management policy, personnel, confidential and financial information, business records access, physical access to facilities, information and communication technologies and their use, document and data management

1. International ISMS Standards

- <u>ISO/IEC 27001, 2005-10-15 Ed. 1</u>
Information technology — Security techniques —
Information security management systems — Requirements

- <u>ISO/IEC 27002, 2007-07-01 Ed 1 (ISO 17799 2005-6-15 Ed 2)</u>
Information technology — Security techniques — Code of practice for information security management

- <u>ISO/IEC 27006, 2007-07-01 Ed 1</u>
Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

- Under development: <u>ISO/IEC CD 27005</u>
…. Security techniques — Information security risk management

2. Supply Security Management Systems (SSMS)

- Formalize supply security, provide harmonizing platform

- Transport and customs perspective—movement/access

- Scope defined by organization and commercial agreements

- Focus: supply and transport security, risk exposure, response

- Affects

  - Physical access to facilities, freight security and monitoring, personnel, confidential and financial information, business records access, document and data management

2. International SSMS Standards

- <u>ISO/PAS 28000, 2005-11-15 Ed. 1</u>
  Security management systems for the supply chain

- <u>ISO/PAS 28003, 2006-10-01 Ed. 1</u>
  Security management systems for the supply chain—
  Requirements for bodies providing audit and certification of supply chain security management systems

- <u>ISO/IEC 28004, 2007-10-15 Ed. 1</u>
  Security management systems for the supply chain – Guidelines for the implementation of ISO 28000

- <u>ISO/DIS 28001, (2007 ISO TC 8/SC 11)</u>
  Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance

See www.iso.org

1+2. Information and Supply Security

- North American Security Products Organization (NASPO)

  - American National Standards Institute (ANSI) accredited Standards Developer

- ANSI/NASPO–SA–2008

  - Security Assurance Standards for the Document and Product Security Industries

- US National Security Assurance Standard, see www.naspo.info

- Impacts both information and supply security management systems

- ANSI/NASPO proposal for an ISO Fraud and Countermeasures Technical Committee (TC) was approved Jan '09 creating TC 247

See www.naspo.info

3. Authentication

- Developed arena

  - Overt methods: optically variable devices (color shift, holograms), intaglio, labels, markings, etc

  - Covert methods: taggants, invisible markings, DNA, micro-tags, nanotechnology, and forensic analysis

- Multi-layer approach has become the default

  - Keep changing out elements as counterfeiters catch up

- Past: internally motivated implementation

- Future: legal or commercial requirement for market access

3. Authentication: New Dimension

- Additional technique being adopted globally, termed

    - Mass Serialization (MS)

    - Product Control and Authentication (PCA)

    - Digital Authentication (DA) (compared to Sensory)

- Securely connect products, people, documents, or processes to the Internet to support authentication

3. Authentication: Evolving Numbering Approaches

- Simple numbers: 12345…12346….12347……

- Data embedded numbers: 080402 624 42134 123Q2N627

        Production Date   Plant   Shift   Batch   Product   Serial

- Secure, unique codes   3j214i038og3

    - Securely generated codes and secure platforms

    - Codes link to authentic record containing original data

        - Data parameters and access controlled by client

3. Authentication: Secure, Unique Codes

- Can be added to existing stream of identifiers or be used as a substitute (serial number as secure code)

- Codes added to supply—product, package, case, document, etc

- Authentication available at any point in lifecycle—from supply through customs, distribution, retail, and final owner or consumer

- Authentication possible through the following:

  - - Computer and Internet browser
    - Mobile phone: SMS
    - Mobile Internet—character entry or 2D bar code

- Codes may be overt, covert, both, and/or associated

Use and Source of Secure Codes and Platforms

• Nokia	Proprietary system	Batteries
• GSK	Proprietary system	Pharmaceuticals
• Nike Golf	TUV Rheinland	Golf clubs
• Cardinal Health	SupplyScape	Medical devices
• Lexcom	TUV Rheinland	Automotive parts
• Driscoll's	YottaMark	Agriculture
• Teccom	Vesdo	Automotive parts
• Saudi Arabia	Multiple systems	Import certificates
• US Dept. of Defense	Multiple systems	General supply

- Others: electronics, medical devices, consumer electronics, luxury goods, consumer goods, healthcare, automotive, food and agriculture

What Issues Are Being Addressed By Use?

- Supply security

- Brand Integrity

- Anti-counterfeit

  - Unintended counterfeit purchases*

    - Faster discovery and response time

  - Intended counterfeit purchases*

    - Legal evidence

- Support investigations, interdictions, and seizures

- Support trade intelligence

- Product Control

- Product Recall

*See: http://www.oecd.org/dataoecd/11/38/38704571.pdf

What Issues Are Being Addressed By Use?

- Answer questions

    - Is it ours?

    - What is it supposed to be?

    - Is it where it is expected to be?

    - Authenticated? When and where?

- Leads to track, trace, secure streams, and chains of custody

    - Add timing, process, and association rules

Additional Advantages

- Augments existing approaches easily

- Implementation is simpler than most alternatives

- Scalable

- Adaptable

- Resource and strategy coordination
  - Brand Risk Management team
  - Enterprise
  - Suppliers
  - Customs
  - Resources and vendors
  - Distributors
  - Retailers

# Additional Advantages

- Continuity over time

Illustrative example

	Year 1	Year 2.5	Year 4.5
Optically Variable Device	Hologram A	Hologram B	Color shift
Covert marking	UV	Invisible bar code	Micro/nano markers
Covert forensic	Specialty ink A	Specialty ink B	DNA
Unique, secure codes	Codes	Codes	Codes

Authentication platform

Client-controlled, multi-party access
- Suppliers
- Distributors
- Retailers
- Customs
- Investigations
- Consumers
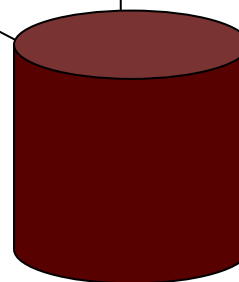
Mass Serialization Regulations and Standards

- US Food & Drug Administration (FDA): Notice of Proposed Rule Making (NPRM) affecting medical devices (Nov '06)

- US FDA pharmaceutical maker user fees NPRM (May '07)

- US Department of Defense Unique Identification Policy

- ANSI proposal for an ISO Fraud and Countermeasures Technical Committee (TC) was approved Jan '09 creating TC 247 with NASPO as Secretariat

- ISO PC 246: "Performance requirements for purpose-built anti-counterfeiting tools"

Mass Serialization Regulations and Standards

- Semiconductor Equipment Materials International (SEMI) and Semiconductor Industry Association (SIA)

  - Working jointly and in tandem on authentication standards

  - SEMI US and SEMI Japan Traceability Committees have each formed an Anti-Counterfeit Task Force (ACTF)

  - European SIA has an established ACTF

  - SEMI US: Four proposed standards through initial ballot

    4486 System architecture (re-numbered SEMI T20 at ballot)
    4487 Labeling (Proposed as SEMI T20.1--in review Q109)
    4488 Communications
    4489 Authentication Service Provider Qualifications
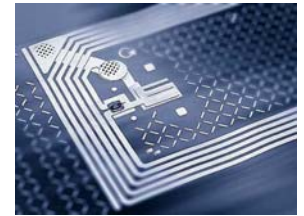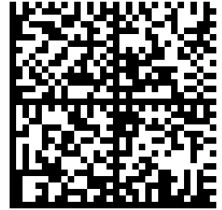
More on Mass Serialization's Secure Codes

- Secure, unique alpha-numeric codes

  - Difficult, expensive, and time-consuming to crack code generation algorithm

- Secure platform to execute and manage authentication

  - Positively identify codes generated by system

  - Data parameters set by client, tailor to different groups

- Code generation models vary

  - Secure Hash Algorithm (SHA)

  - Proprietary

More on Mass Serialization's Secure Codes

- Secure codes are carried by some means

    - Example: label, print, or marking

- Secure codes are formatted based on carrier

    - Overt: bar code, 2D bar code, print, label, mark

    - Covert: invisible bar codes; DNA, micro, and nano markers

Product Control and Authentication (PCA)

- Codes are incorporated into production

  - Printing, labels, engraving, marking, tags, etc.

  - Multiple formats:

    - Linear bar codes, 2D bar codes, RFID, etc

GH724ce25299c

TÜV Rheinland Group

0648718643
15H7zuTf7

Authentication: www.tuvbrandprotection.com

Product Control and Authentication (PCA)

- Secure codes are confirmed by

  - Computer Web browser

  - Mobile text message—Simple Messaging System (SMS)

  - Smart phone Web browser

  - In-line and in-process systems

  - Proprietary readers

- Verification message and content controlled by clients

- Multiple language support

PCA Enables Secure Trade Streams

- Tailored workspace

  - Specify processes, transaction and check points, data, and format

  - Programmable process, timing, and channel parameters

  - Hierarchical, associated, or chained codes

  - Enable or disable authentication to match needs

- System access and use records provide basic tracking and tracing

  - Confirm expected events occurred

  - Flag unexpected events for investigation

- Tailored reporting: generic, pre-defined, or user-defined

About TUV Rheinland

- 137 years of objective independence

- Global Assurance Services innovator

- Leading test, certification, and audit provider

- 'Sicherheit' means safety and security

- 13,000 employees, 400 offices, 61 countries

- More than U $1.1 Billion revenue

- http://www.tuv.com/de/en/about_us.html

Trade Cycle Framework…

Supply Network

Consumer Electronics
Home & Appliance
Tools, Lawn, Garden
Audio/Video/Multimedia
Fitness, Sports, Health
Entertainment & Amusement
Medical Devices
Scientific Instrumentation
Information Technology
Communication Technology
Wireless Technology
Laser & Optics Technology
Software
Office Equipment
Semiconductor
Process Control
Machinery
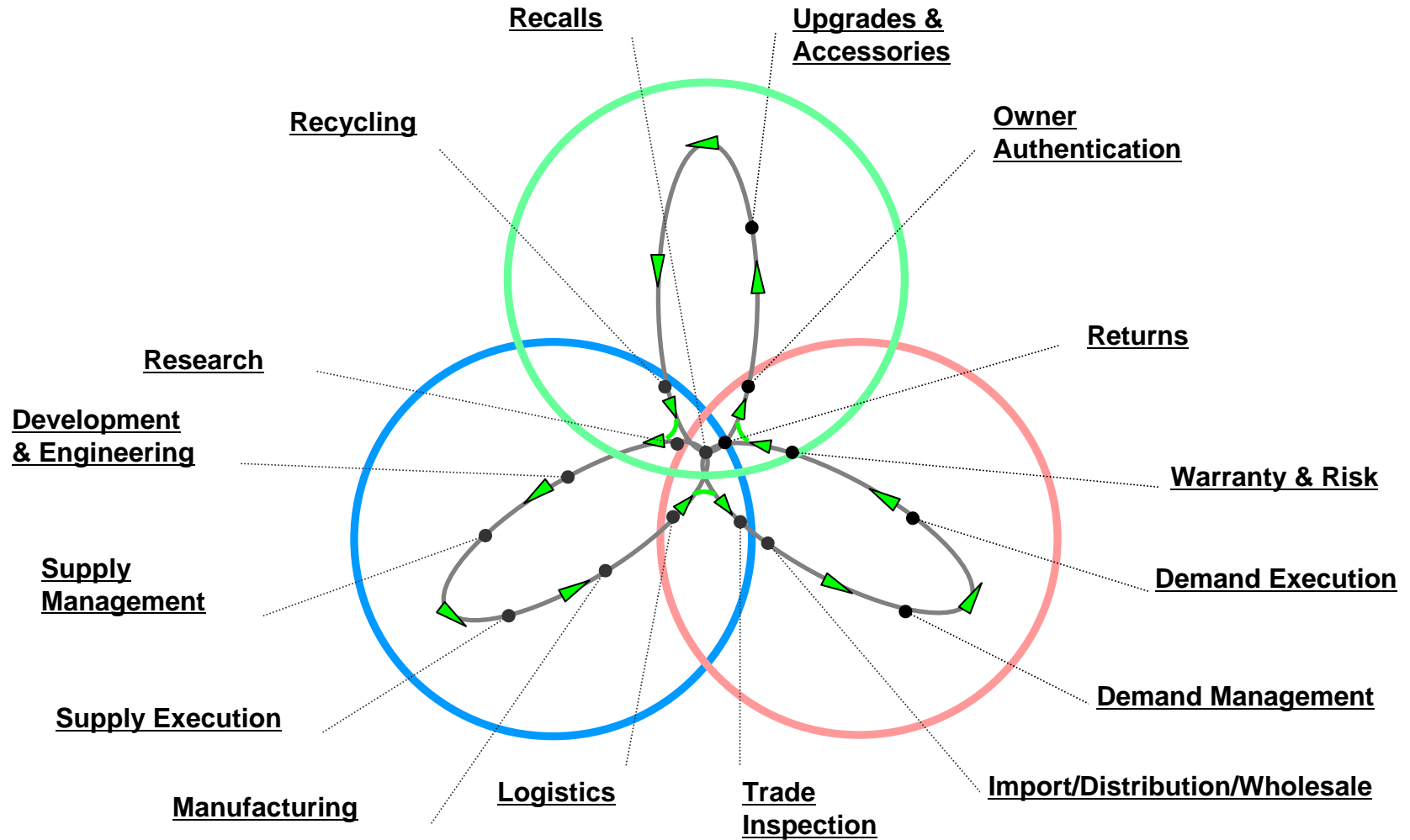Power Distribution
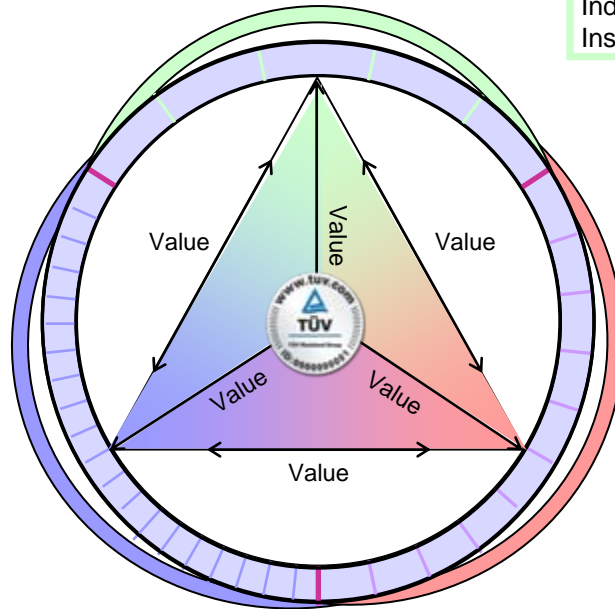
Owners Network

Consumers	Business
Industry	Government
Insurance	Education

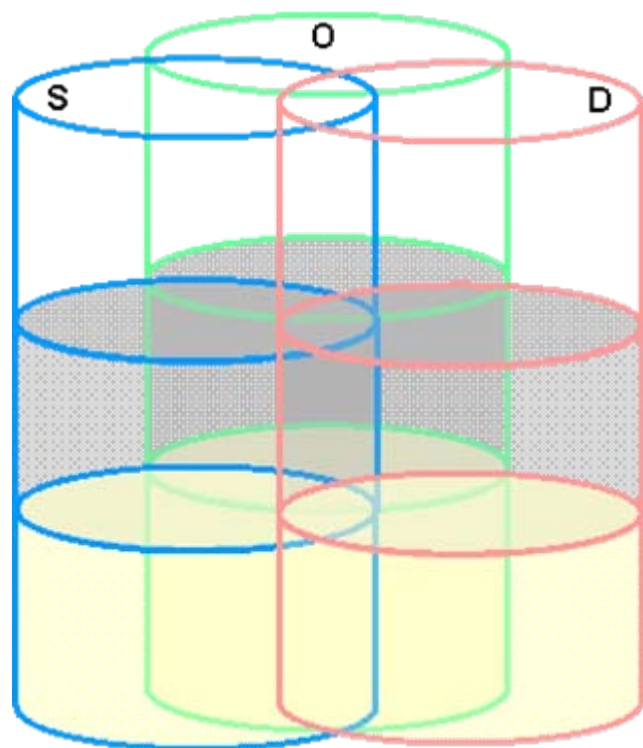|	
- Entertainment	- Retail
- Technology	- Healthcare
- Manufacturing	- Small
- Aerospace	Business
- Semiconductor	- Transport
- Machinery	- Institutions
- Federal, State, &	
Local government	

Demand Network

Retail   Sourcing
Distribution   Import/Export
Procurement   Direct Market/Sale
Exchanges   Hubs & Auctions
OEM/ODM = **O**riginal…
  OEM…Equipment Manufacturer
  ODM…Design Manufacturer

...enables Lifecycle View

Recalls

Upgrades & Accessories

Recycling

Owner Authentication

Returns

Research

Development & Engineering

Warranty & Risk

Supply Management

Demand Execution

Supply Execution

Demand Management

Manufacturing

Logistics

Trade Inspection

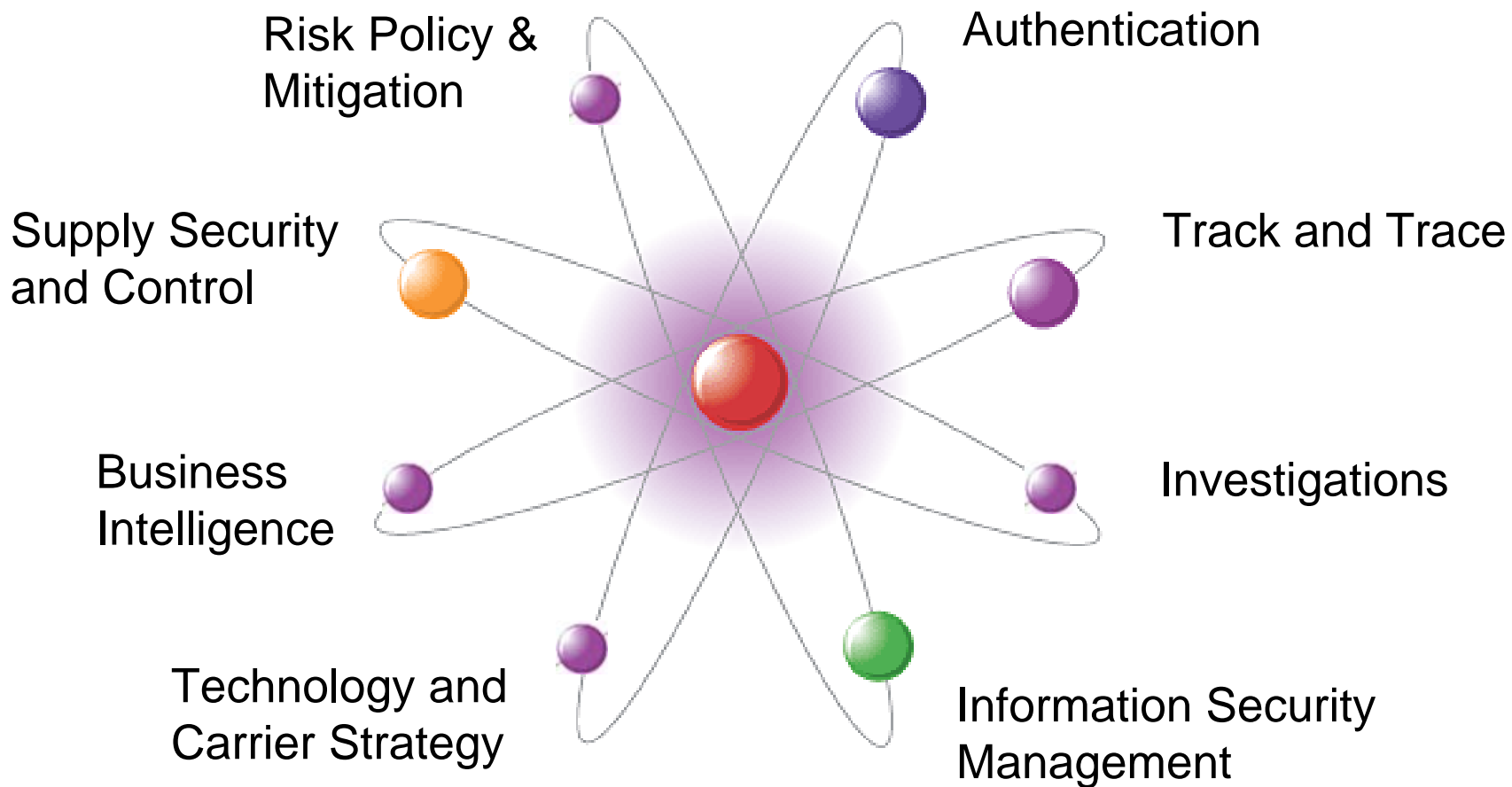Import/Distribution/Wholesale

Three Market Factors

- **Performance**
  Distinguishing benefit: product,
  process, service, and/or characteristic

- **Commercial Access**
  Additional market-driven, demand
  channel, or customer requirements

- **Legal Access**
  Public policy requirements and
  means of implementation enabling
  legally sanctioned products, processes, or services onto
  a market

Market Access

Multidimensional Strategy Required

Risk Policy & Mitigation

Authentication

Supply Security and Control

Track and Trace

Business Intelligence

Investigations

Technology and Carrier Strategy

Information Security Management

TUV Rheinland Group Standing: Security Assurance

- Charter Member, North American Security Products Org. (NASPO)

  - NASPO Class II certified

- Founding Member: International Authentication Association (IAA)

- Authorized US Department of Homeland Security (DHS) auditor for Customs-Trade Partnership Against Terrorism (C-TPAT) pilot

- Authorized EU Customs auditor (EC No. 648/2005)

- Certification body

  - ISO/IEC 27001: Information Security Management Systems

  - ISO 28000: Supply Security Management Systems

TUV Rheinland Group Standing: Security Assurance

- Member, International Anti-Counterfeit Coalition (IACC)

- Member Semiconductor Equipment Materials International (SEMI)

  - Anti-Counterfeiting Task Force (ACTF)

- Member, Coalition Against Counterfeiting and Piracy (CACP)

  - Ant-counterfeiting and Piracy Summit sponsor

- Business Action to Stop Counterfeiting and Piracy (BASCAP) supplier

Information and Supply Security

- Complete supply network security assessments

- Information Security Management System audits: ISO/IEC 27001

- Supply Security System audits: ISO 28000

- US DHS C-TPAT audits

- EU Customs Code (EC No. 648/2005)

- US NASPO AS v3.0 expertise
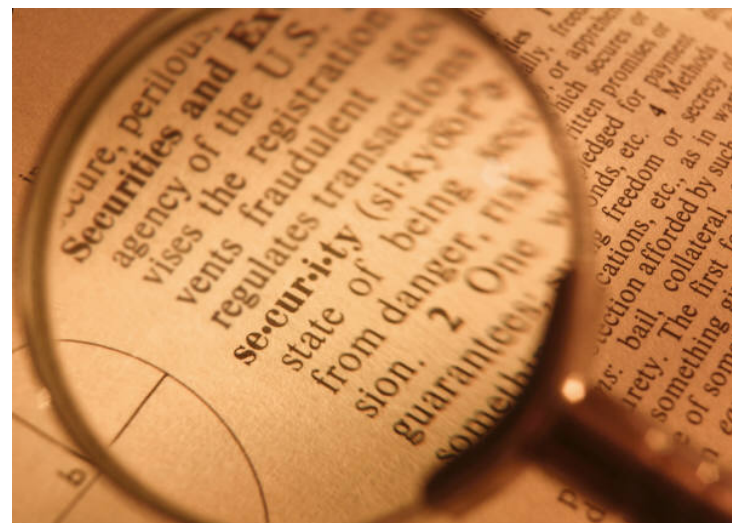
Partner Services

- Investigations

  - Supply Security preparation

  - Field work and Customs relations

  - Background checks

- Internet Monitoring

- Secure Printing and Labels

- Optically Variable Devices and Secure Foils

- Micro, Nano, and DNA markings and markers

- Overt and covert solutions from
  Mutual Development Partners
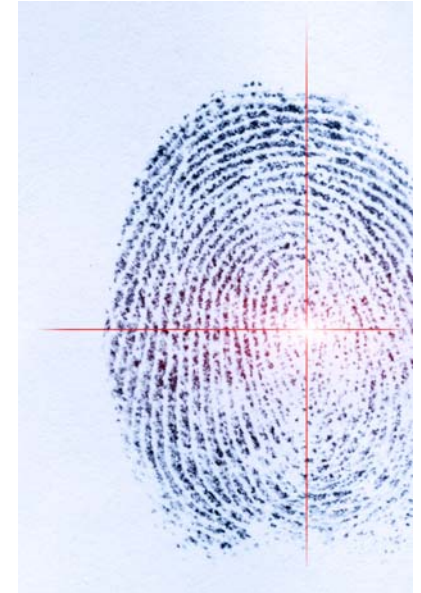
More information:

See: www.brm.tuv.com

or

Email: panger@global.tuv.com
gene.panger@jpn.tuv.com
925 699 1780