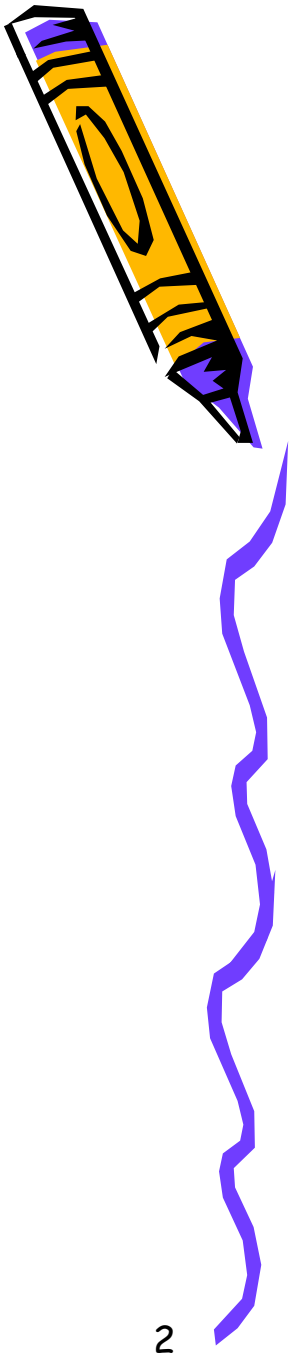
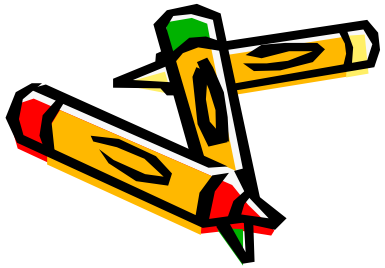
Dutch Lawful Interception and Retained Data Situation

Dutch Ministry of Justice
Koen Jaspers

Ministry of Justice Challenges:

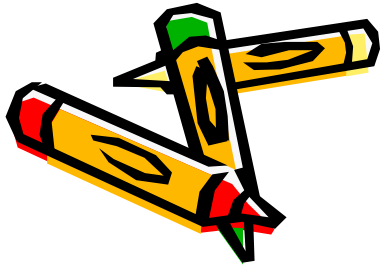


- How can we keep up with the Internet?
  - Monitoring facilities, Social Networks, Nomadic Users, Service and Access
- How to keep education in pace?
  - Detectives, Prosecutor and Court
- How should we (re)define provider?
- How to keep standards in pace?
- How can a Broker be successful?
- Will encryption make LI useless?



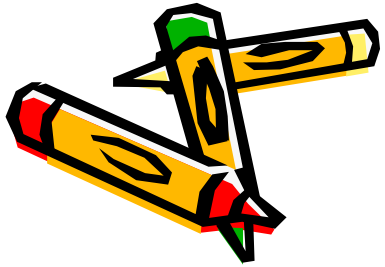
Overview

- History
- Legal frame work
- Standardisation process
- Architectural Approach & Projects
- Lessons Learned & Challenges



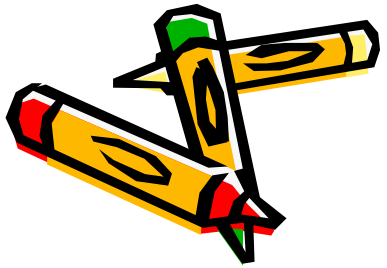
Dutch LI &DR History

- Article 64 '71
  - Provider(s) have to cooperate on lawful interception
  - Government requests and pays implementations
- GSM act '93
  - GSM providers have to pay for LI implementation
  - Other networks fall still under article 64
- Telecommunication Act '98
  - All providers have to pay for LI implementation
  - Internet becomes telecommunication
- Data Retention Act 2009
  - Limited to EU Data Retention Directive



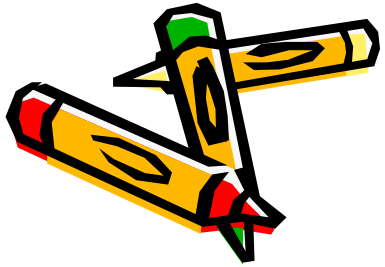
Dutch LI History

- Fixed Telephony
  - 70's access based
  - 2003 service based
- Mobile networks
  - Early 90's analogue networks, service based
  - Mid 90's GSM, service based
- Internet 2001
  - Access: dial up, xDSL, Hot spots, GPRS/UMTS
  - email,
  - VoIP

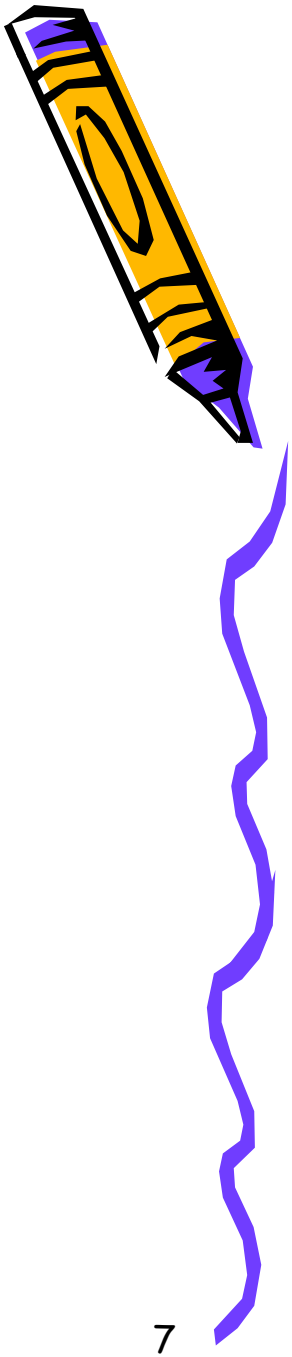


Dutch DR History

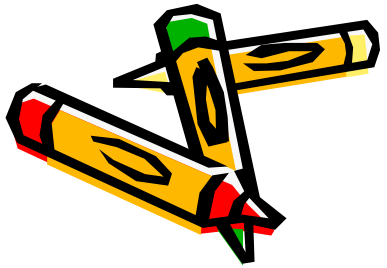
- Till 2004
  - Provider stored information (could go back to the start of service)
  - Many formats
  - Good & poor accessible (electronic and micro fiches)
  - Mainly Fixed & Mobile Telephony networks
- 2004 to 2009
  - EU Privacy Directive in place
  - Information necessary for business provider
  - Fixed & Mobile Telephony networks 3 to 7 months
  - Internet very limited
- From September 2009
  - Telephony and Internet one year
  - Limited practical implementations



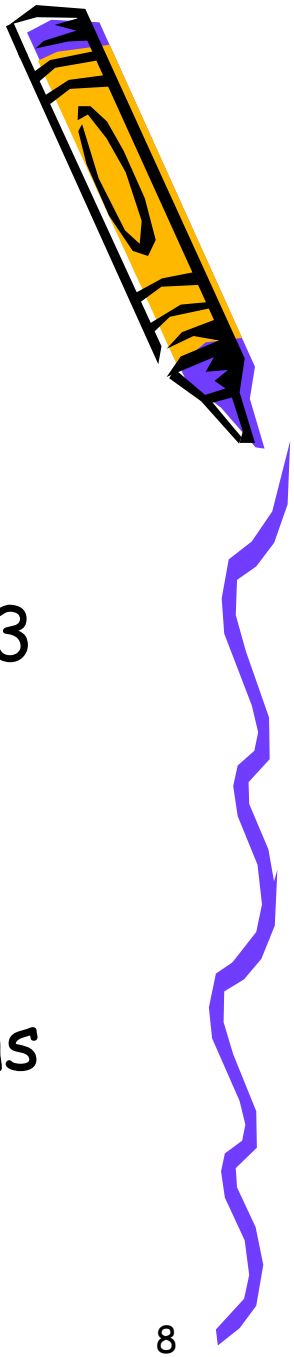
Dutch Legal Framework Involved Acts



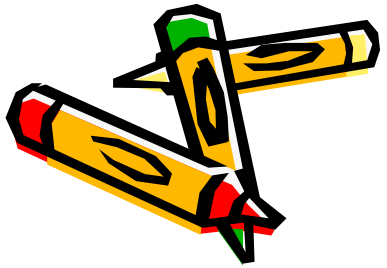
- Code of Criminal Procedure
  - Permitted for investigations
- State Security acts
  - Permitted for security & intelligence
- Telecommunication Act
  - LI & DR Obligations providers



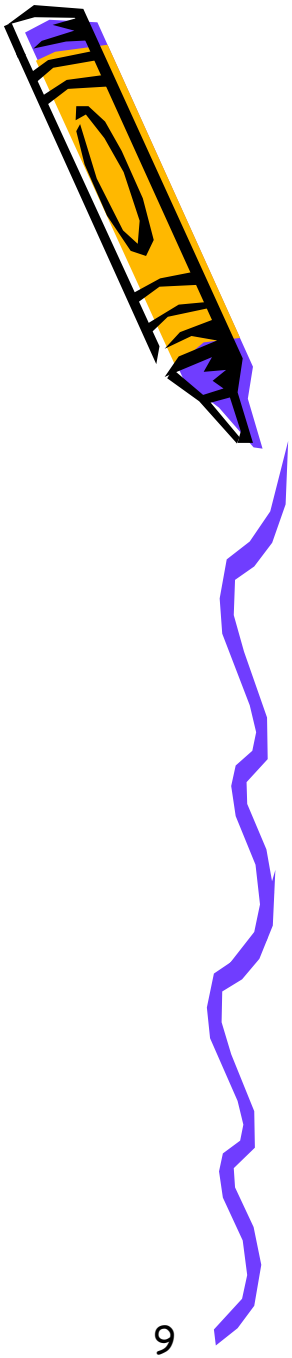
Dutch Legal Framework Involved Acts



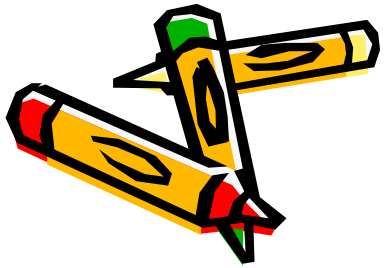
- Mirror paragraphs
  - Obligation vs Permission
  - Telecommunication Act'98, chapter 13
  - Code of Criminal Procedures
  - Intelligence Service Act
- Lower Regulation
  - Limitative Obligations and Permissions



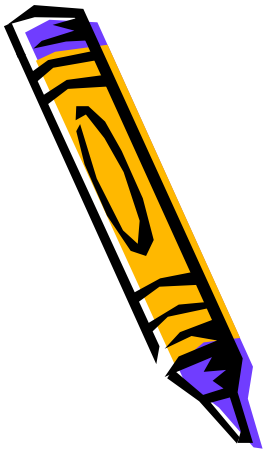
Dutch Legal Framework Levels of Privacy Intrusion



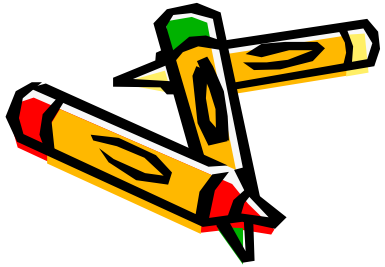
- Directory Numbers vs Names
- Traffic analyses
  - numbers
    - target/victim
    - GSM, PSTN, email, IP-access
  - location
    - Calls made at base stations near location crime
- Lawful Interception
  - target/victim



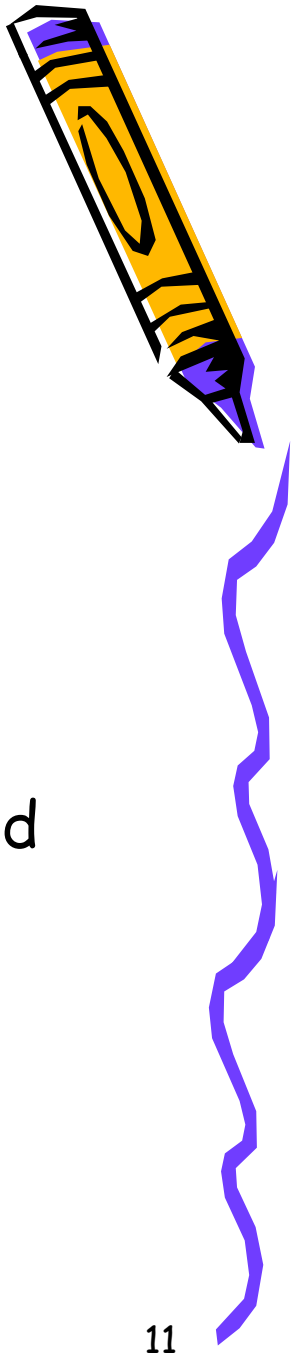
Dutch Legal Framework
Code of Criminal Procedure



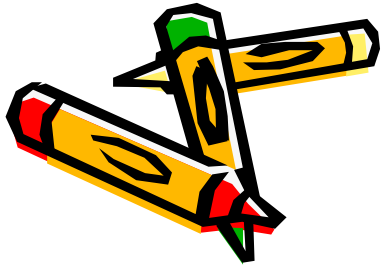
- Lawful Interception for what:
  - Crimes > 4 years imprisonment (no bail)
  - Life threatening situations
  - Finalise investigation, evidence guilty not guilty
- Lawful Interception procedure:
  - Warrant by Prosecutor, checked by Judge Commissioner
  - Proportional: intrusion privacy vs crime?
  - Subsidiarity: other less intrusive tool?



Dutch Legal Framework Code of Criminal Procedure

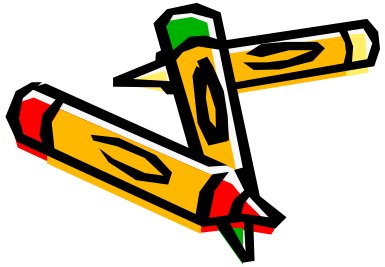


- Retained Data for what:
  - Investigating serious crimes
  - Finding relations, suspects, proof
- Retained Data procedure:
  - Warrant by Prosecutor (afterwards checked by Judge Commissioner)
  - Proportional: intrusion privacy vs crime?
  - Subsidiarity: other less intrusive tool?



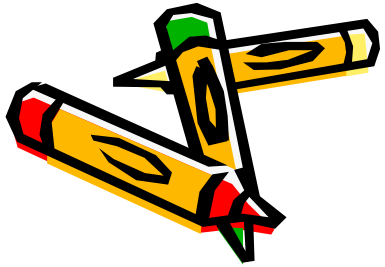
Dutch Legal Framework Code of Criminal Procedure

- Numbers vs Names for what:
  - Criminal Investigations
  - Finding relations number with persons
  - Finding provider for Lawful Intercept
- Numbers vs Names procedure:
  - Demand by senior Investigator (under responsibility of leading prosecutor)



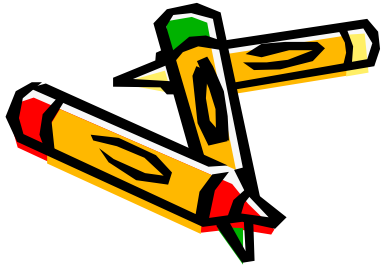
Dutch Legal Framework Code of C. P. Boundaries

- All information also available for defence (public!)
- Information can only be used in the investigation it was requested for
- After final prosecution the information must be deleted
- LI is not a tracing tool, location only at start of communication



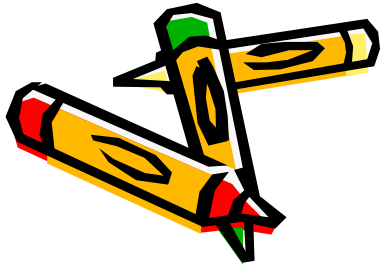
Dutch Legal Framework Telecommunication Act '98

- What: all pubic telecommunications
  - networks and services, includes Internet
- Interceptable at the start of service
- Cost
  - Providers pay for the investment and maintenance
  - Law Enforcement pays personnel & administrative cost for actual intercepts



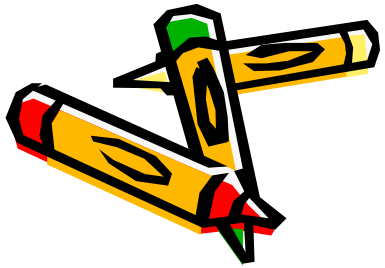
Dutch Legal Framework Telecommunication Act '98

- Enforcement (ch. 13) by Telecommunication Agency (MoE)
- Functional requirements on WHAT to deliver
  - Details on parameters
  - Available in core network
  - No influence on network services or architecture
- Detailed technical specification on HOW to deliver
  - After consultation with the providers the government decides

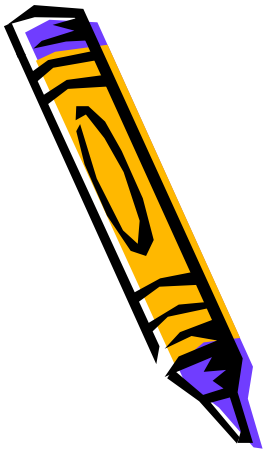


Dutch Legal Framework Functional Requirements

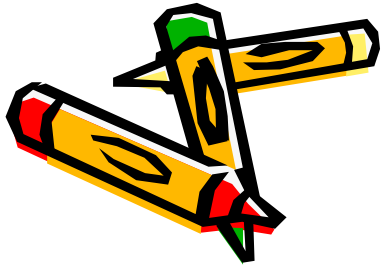
- Trigger for Lawful Interception:
  - Fixed: Directory number(s)
  - Mobile: MSISDN, IMEI, IMSI
  - Internet: IP address, MAC, username, email address



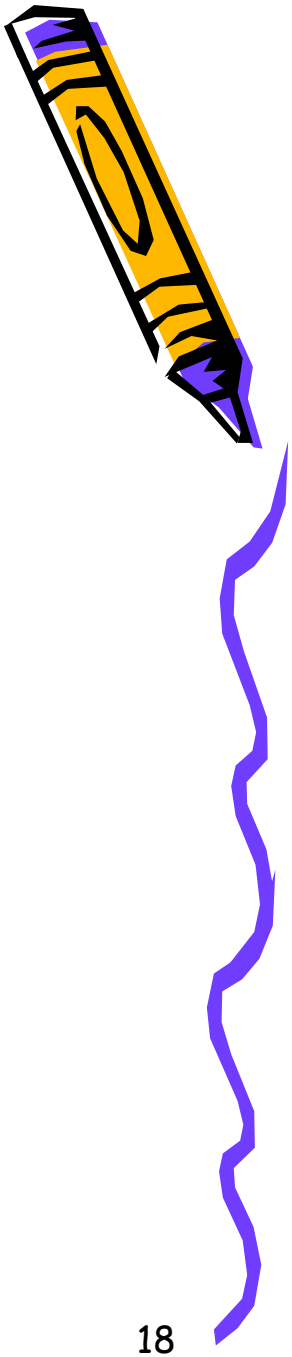
Dutch Legal Framework Functional Requirements



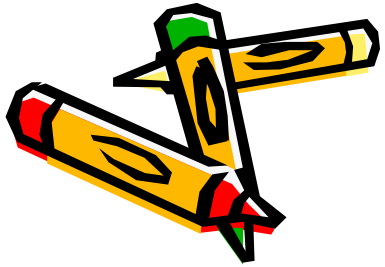
- Intercept Related Information:
  - Fixed & mobile: from-, to-, redirected address, TS&BS as available
  - Mobile: target MSISDN, IMEI, IMSI and location (at start of communication)
  - Internet: log on and log off information (signalling not separated from content)
  - All time stamped



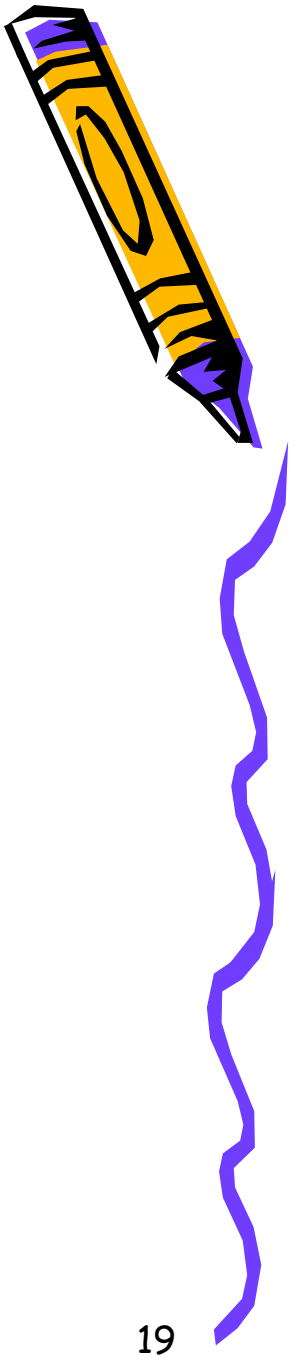
Dutch Legal Framework Functional Requirements



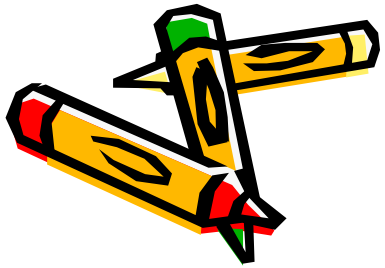
- Content of Communication:
  - Fixed:
    from-, to-, redirected (associated) content
  - Mobile:
    from-, to-, redirected (associated) content
    speech, fax, data, SMS,
    GPRS, MMS, UMTS-CS/PS
  - Internet Access: from- and to target
  - Email: from and to emails



Dutch Legal Framework Functional Requirements

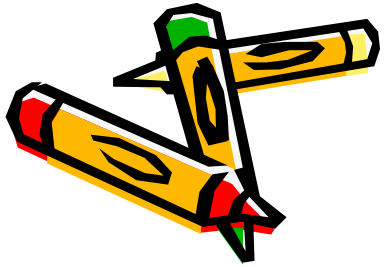


- Security:
  - Reliability personnel & environment provider
  - No access for third parties,
  - Not noticeable for users service
  - No visibility among LEA's and investigations
- Quality
  - Delivery as good as the target service (or better)
  - Audits possible
- Quantity
  - Up to three independent LEA's on one target
  - Multiple targets to best practice



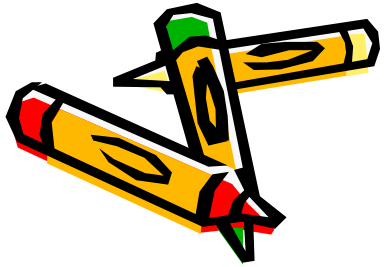
Dutch Legal Framework Functional Requirements

- Activation intercept immediately
  - Normally same day (business hours),
  - Emergency within hour(s) (also outside business hours)
- Delivery intercept
  - IRI as soon as available (normally seconds)
  - Circuit switched (voice) undelayed (< 1 sec)
  - Packet switched (data) within seconds

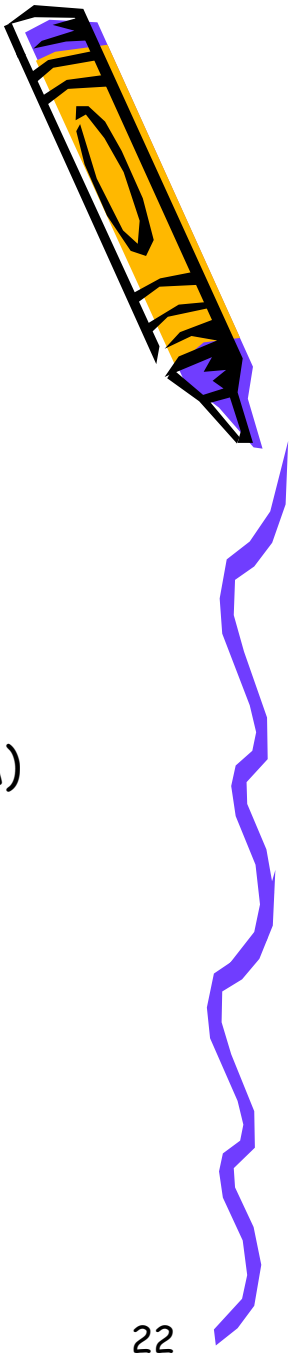


Standardisation Process

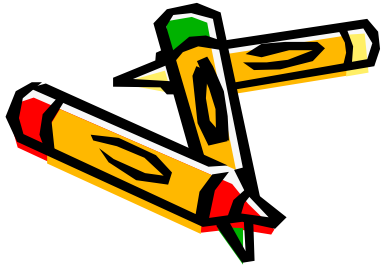
- 70's:
  - Information: subscriber line, access based
  - Delivery PTT developed lease line LI protocol
- GSM 1993:
  - Information ETSI Service based
  - Delivery 'JTS' national development (government & providers) based on ISDN
- Telephony 2000
  - Information 'ETSI' service based
  - Delivery ETSI 201 671 'ETSI-nl' (ISDN/X.25)
- Internet 2000
  - Information packet copies
  - Delivery national development (government & providers) 'TIIT'



Standardisation Process

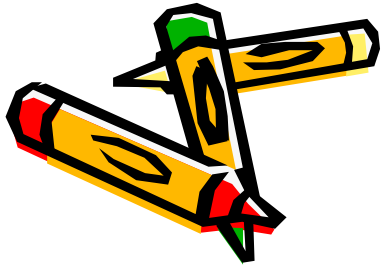


- National LI standards:
  - Limited in features
  - Late with implementing new services
  - Poor detailed knowledge
- Telecommunications (& LI) no longer a national thing:
  - International standards mandatory by EU
  - No national functionality (economically) possible (e.g. GSM)
  - LI is no longer a national matter
- International approach
  - International requirements: IUR'95
  - Participation in international LI standards



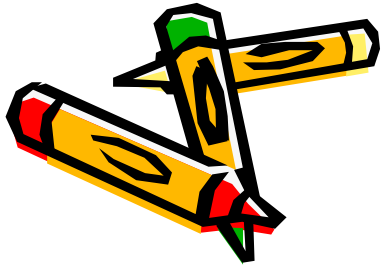
Standardisation Process

- International LI standards:
  - In line with Core Industry road maps
  - In phase with primary services, future services
  - Access to experts and developers
  - Inform industry on LI requirements on future services
  - National awareness of future services



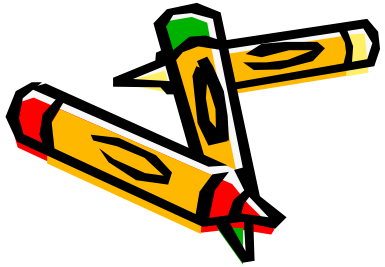
Standardisation Process

- Which standards to participate in?
  - ITU: framework/models, political,
  - ETSI: GSM till 90's, European, LI history, LI supportive
  - 3GPP: GSM, UMTS, LTE, (ETSI) LI history, LI supportive
  - IETF: IP development, 'free' services, non government supportive
  - WiMax: will it take of nationally? LI supportive
  - IEEE: …
  - …
- ETSI TC-LI: Open for Work Items
  - IP
  - Retained Data
  - Dynamic Triggering

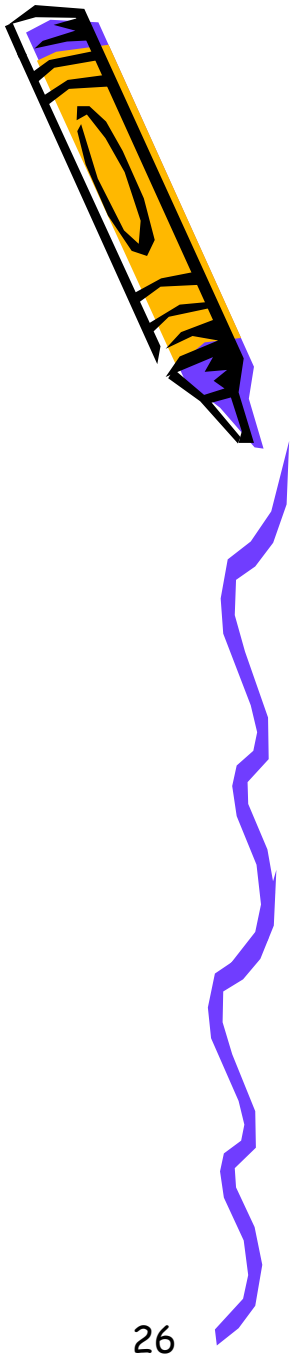


Standardisation Process

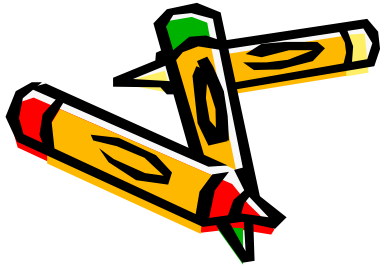
- National use of International LI standards:
- Representation in the international standards
  - Incorporate (national) requirements
  - Prepare national hooks
  - Feed back omissions
- National adaptation
  - National working group
  - Technical and legal
  - Fix options
  - Add national features (e.g. security, transport)
  - 'ETSI-x.nl'
- Done: Fixed & Mobile Telephony ETSI 201 671: ETSI-nl
- Prepared: Internet ETSI 102 232: ETSI-ip.nl
- In preparation: Retained Data ETSI 102 656: ETSI-dr.nl



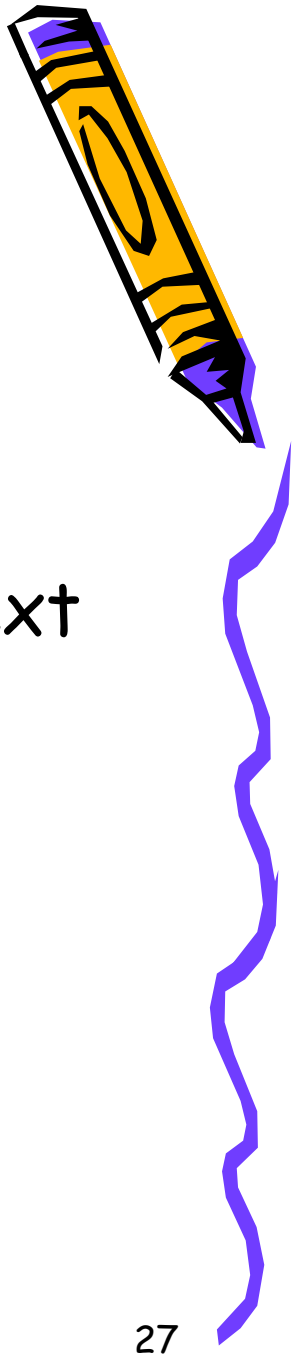
Architectural Approach & Projects



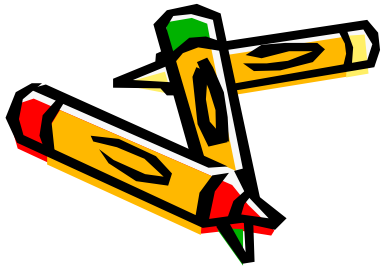
- Early 90's
  - One provider
  - Service: Telephony
  - Many Law Enforcement Agencies
  - Many simple Monitoring Facilities
- Mid 90's
  - Many providers
  - Many services:
    - PSTN, GSM, SMS, UMTS, IP, Cable, xDSL, email
  - Many Law Enforcement Agencies
  - Many too simple Monitoring Facilities



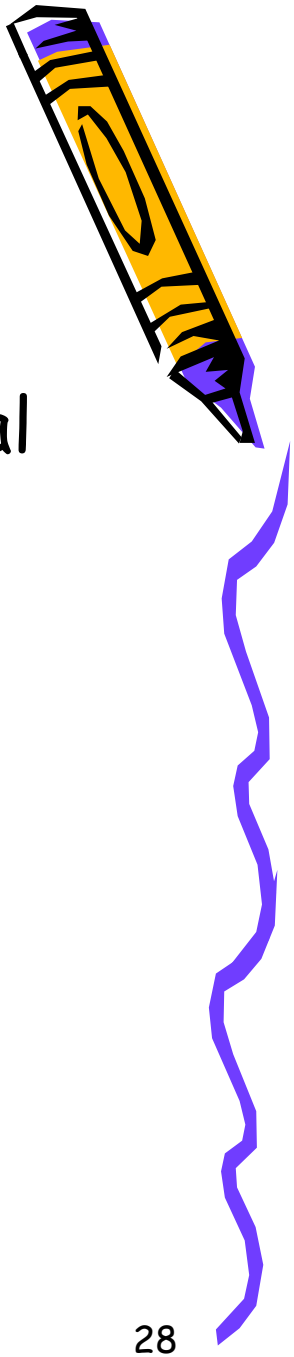
Architectural Approach & Projects



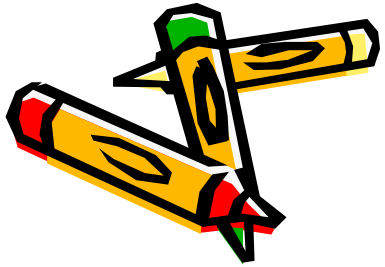
- Telecommunication Act '98
  - Li organised for all providers
- Organisation on government side the next bottleneck
- Coordination needed:
  - Centralisation Investments
  - Centralisation Expertise
  - Broker Function(s)



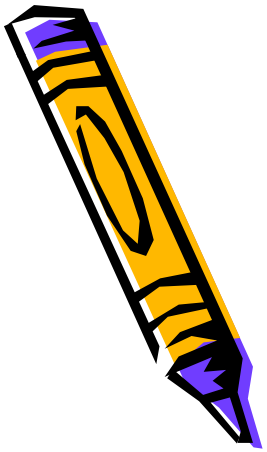
Architectural Approach & Projects



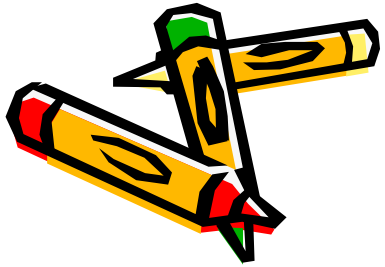
- Platform Interception Decryption Signal analysis (PIDS, 2000)
  Cooperation on:
  - Ministries, policy
  - Law Enforcement Agencies, Intelligence Agencies
  - Central point for providers
  - International contacts
  - Projects



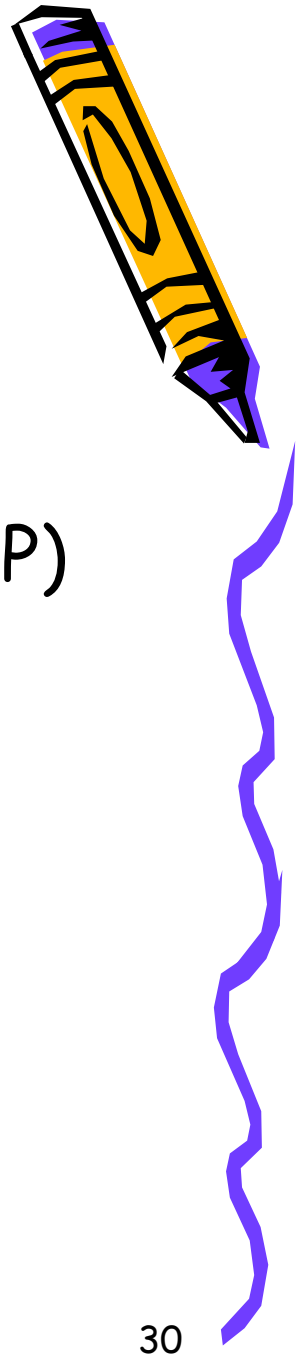
Architectural Approach & Projects



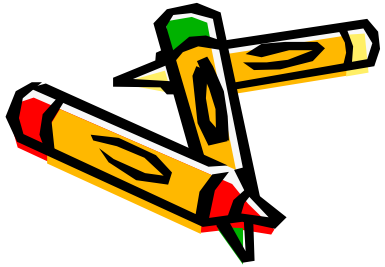
- Central Subscriber Database (CIOT, 2000)
  - Number portability
  - Sub set of all Subscriber databases every 24 hours
  - Access to the relation of
    - Provider
    - Name, Address
    - Service Identifier (phone number, IMSI, IMEI, IP address, email address)
    - Service Subscription Information



Architectural Approach & Projects

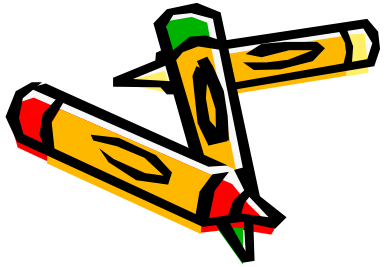


- Many Monitoring Facilities
  - Fast developing services (e.g. GSM, IP)
  - Limited local expertise
  - Limited budgets
  - Chaotic relations LEAs vs Providers
  - Broad bandwidth in Quality

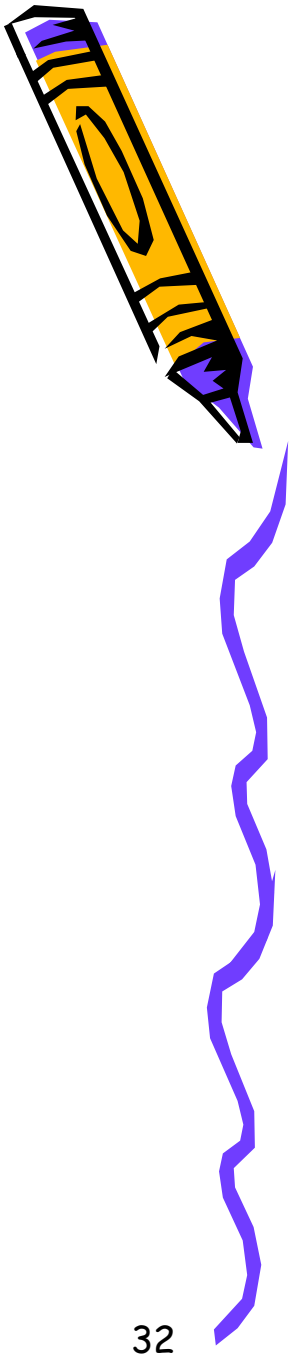


Architectural Approach & Projects

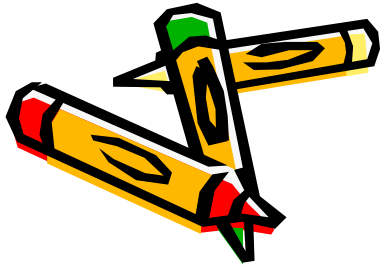
- Concentration Monitoring Facilities (ULI, I&SS, 2004)
  - Broker function LEAs, Providers
  - Expertise centre
  - Manageable level of technical facilities
  - Central gateways for delivery (telephony & IP)
  - Limited number of analysis facilities
  - Local access to 'enhanced' information



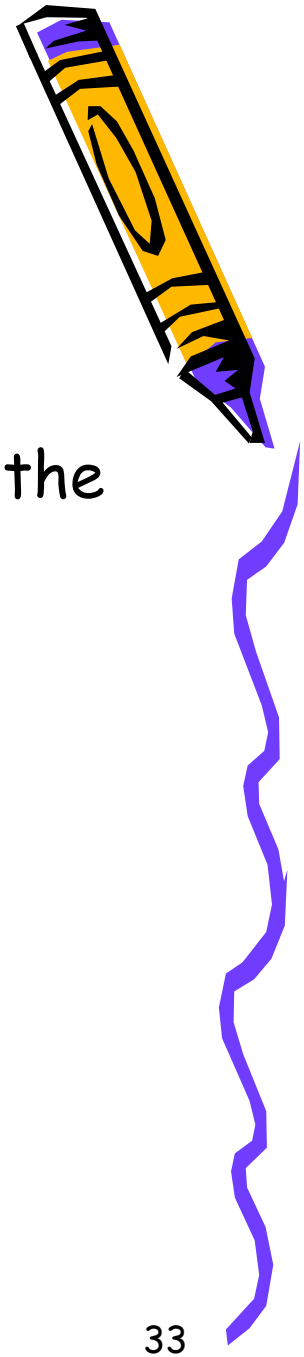
Architectural Approach & Projects



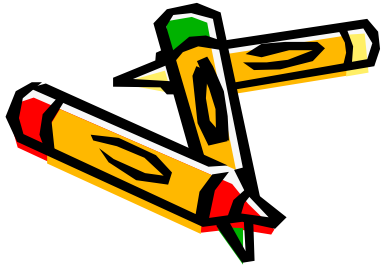
- Electronic warrant
  - Current paper (fax) warrant
    - Verification,
    - Complete,
    - Correct
    - Manual processes
  - Legislation in preparation
  - ETSI TC-LI work item
  - Tools available



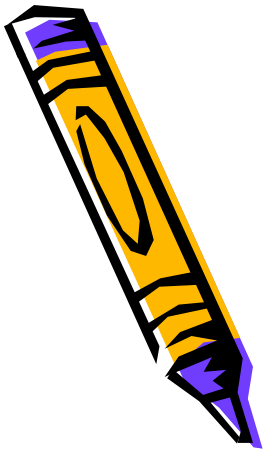
Lessons Learned & Challenges



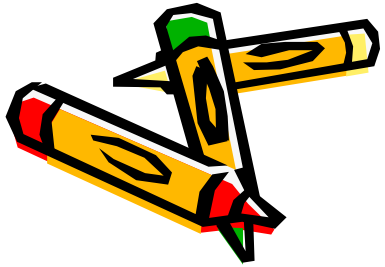
- Concentration monitoring facilities limits the bandwidth in quality. On the lower but also at the upper side. Should all technical analysis be centralised?
- IP still not under control
  - Diversity in services
  - Fast development
  - Social networks
  - Poor commercial LI products
  - To much information for the investigator
  - How to transcribe or how to bring it to court



Lessons Learned & Challenges

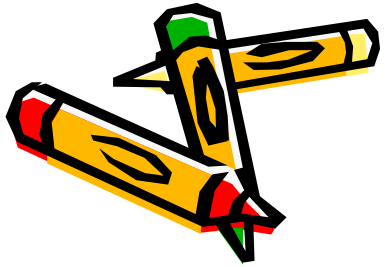


- How to define "provider"
  - Where ends telecommunication and starts application
  - All (IP) providers must be interceptable but do we address all providers with warrants
- Broker function
  - Phonebook & Monitoring facilities
  - Retained Data
  - Non telecommunication market
- Expertise
  - Education and Knowledge level of average detective
  - To little specialised "Digital" Detectives



Lessons Learned & Challenges

- Service and Access unbound: Dynamic Triggering
  - Typical example VoIP Telephony
  - Service provider and Access Provider separate
  - Service provider no access to the content
  - Access Provider no relation to the service
  - Nomadic subscriber
  - No legislation yet
  - ETSI TC-LI work item
- Enforcement of standards and versions
- Encryption: Provider Involved vs full End to End



Thank you!

Questions?