

# DNS INFRASTRUCTURE AND DNSSEC OVERVIEW, PERSONAL DATA PROTECTION IN .LT DOMAIN

KTU ITD Internet Service Centre, dba Domreg.lt  
T. Mackus, D. Tamulionienė

6th International conference for ccTLD registries and registrars of  
CIS, Central and Eastern Europe

2013-09-12  
Crete





# DNS INFRASTRUCTURE



# DNS SERVERS

- .LT DNS servers:
  - a.tld.lt - IPv4, unicast, few redundant servers
  - b.tld.lt - IPv4, IPv6, anycast, 3 locations
  - c.tld.lt - IPv4, IPv6, anycast, 42 locations (CommunityDNS)
  - d.tld.lt - IPv4, IPv6, anycast, 4 locations
  - e.tld.lt - IPv4, IPv6, anycast, 2 locations
  - f.tld.lt - IPv4, IPv6, anycast, 2 locations (ongoing development)

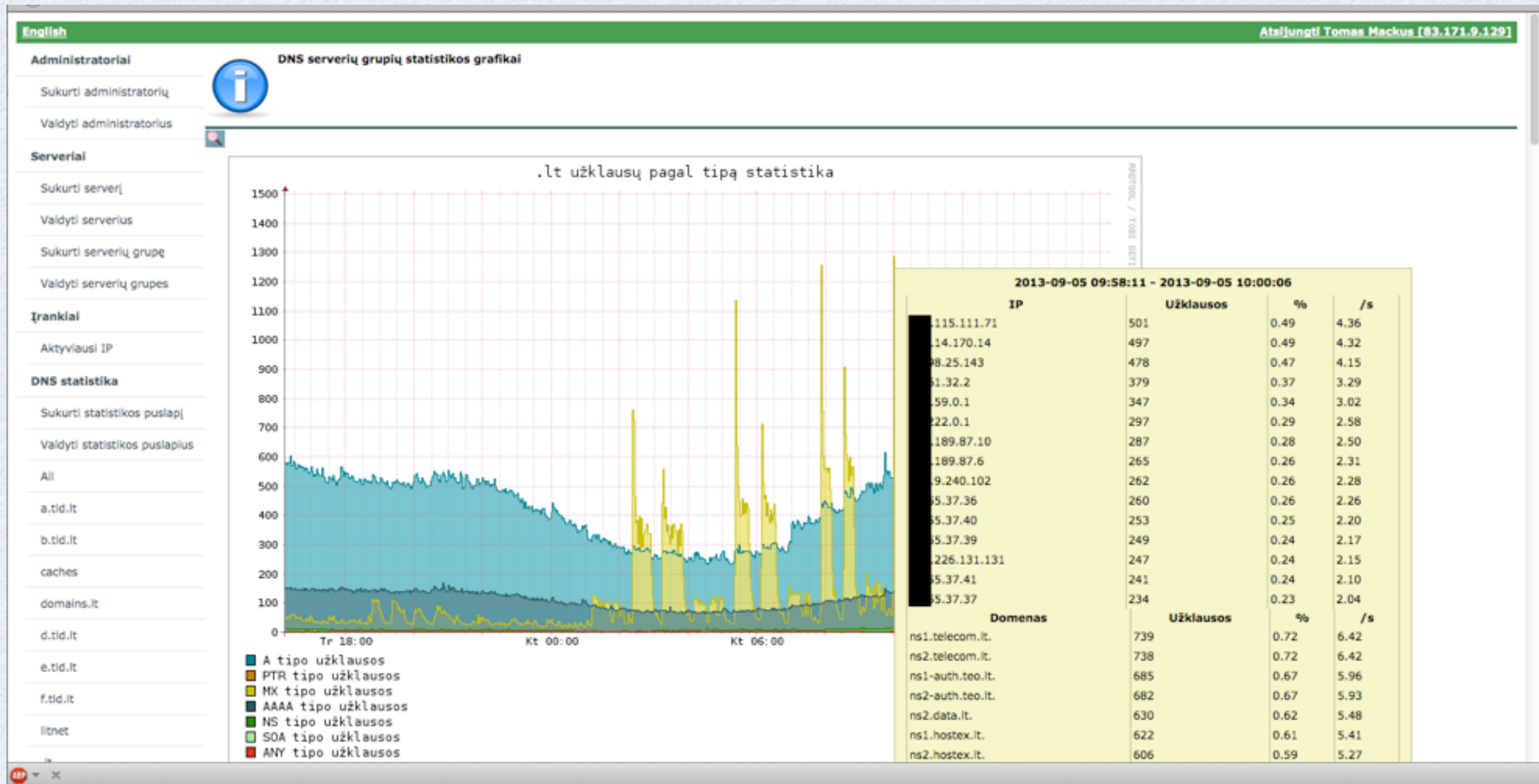


# MONITORING

- Server / services monitoring using ICINGA (NAGIOS)
- Statistics (CPU, memory, network, etc.) monitoring using CACTI
- DNS traffic monitoring using proprietary software (SQLite for logs, RRD for graphs, PCAP / NFLOG for packet capture)



# DNS TRAFFIC MONITORING





# DNS PROTECTION

- Firewall based DNS protection using **xt\_dns** and **xt\_hashlimit** for **iptables**
- Response Rate Limiting (RRL) add-on to **BIND** and **NSD** DNS servers.



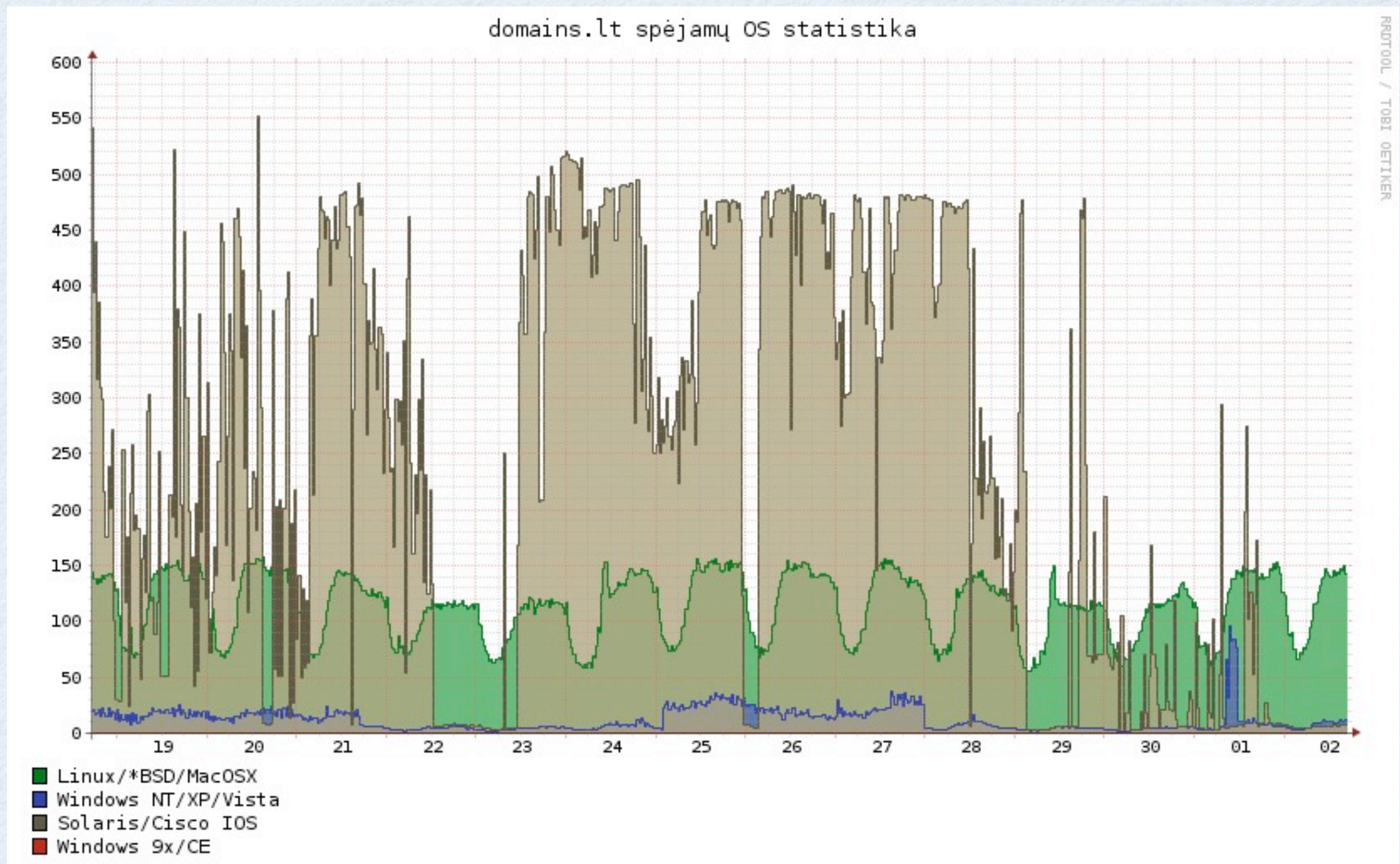
# DNS QUERIES BY TYPE

domains.lt užklausų pagal tipą statistika





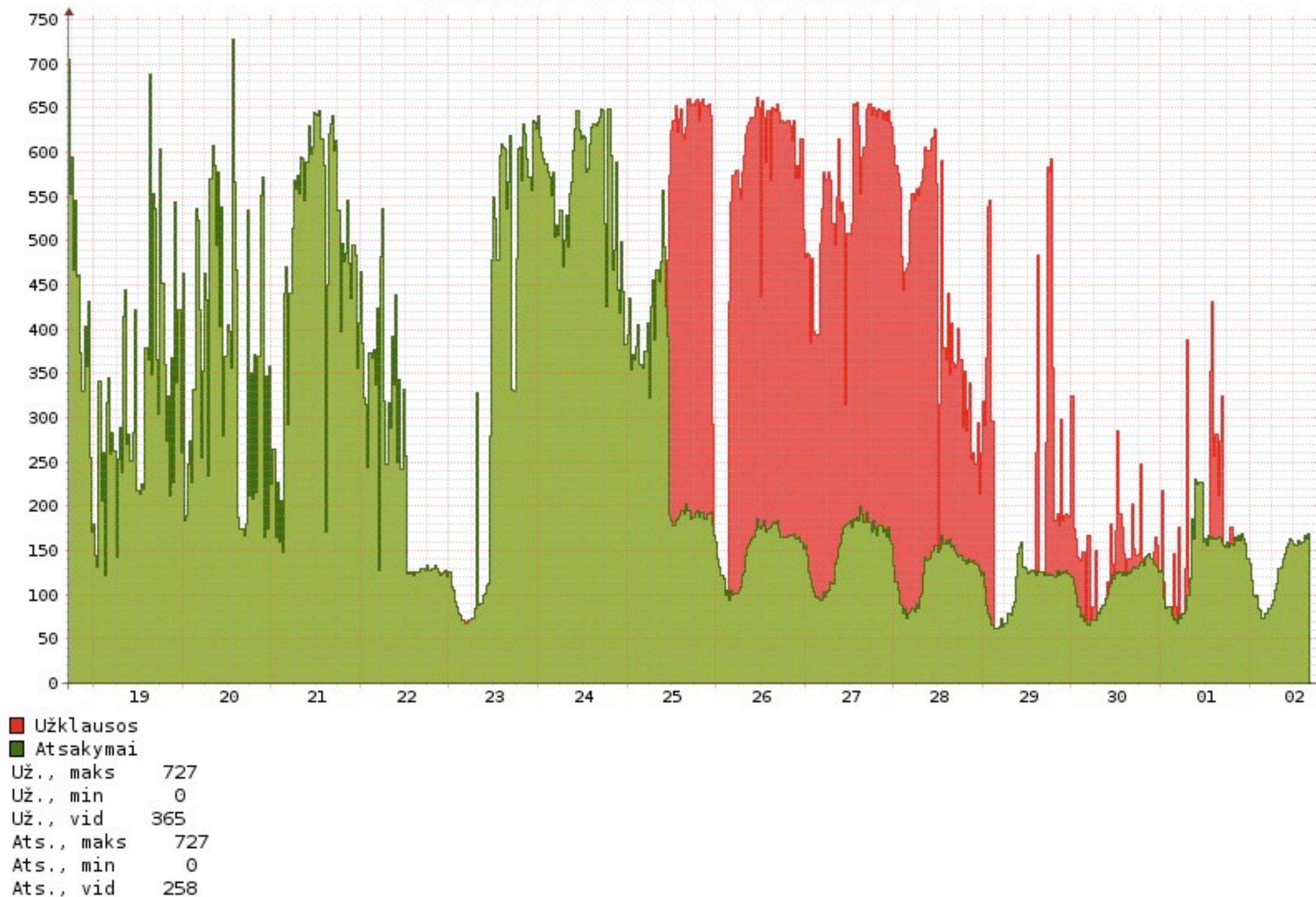
# DNS QUERIES BY TTL





# DNS QUERY LIMITING

domains.lt užklausų/atsakymų statistika





DNSSEC IN .LT



# .LT DNSSEC REALIZATION

- FIPS 140-2 level 3 HSM used for signing.
- Interface with HSM using PKCS#11
- Real world 400 RSA 1024bit signatures per second.
- Private key can be transferred to new HSM only using 3 of 5 smart-cards.



# .LT DNSSEC PARAMETERS

- **KSK :**
  - RSA / SHA-256 encoding algorithm
  - 4096bit length
  - Changing every year
- **ZSK :**
  - RSA / SHA-256 encoding algorithm
  - 1024bit length
  - Changing every month
  - Use of NSEC3 with OPT-OUT
    - SALT (10B) with 5 iterations used for HASH. SALT change every 24h.



# .LT DNSSEC RECORDS

- DS records can be entered together with .lt domain delegation (NS) records:
  - DS key ID (KEYTAG)
  - Algorithm (DSA/SHA1, RSA/SHA1, DSA-NSEC3-SHA1, RSASHA1-NSEC3-SHA1, RSA/SHA256, RSA/SHA512)
  - HASH type (SHA1, SHA256)
  - HASH



# .LT DNSSEC TIMELINE

- 2012-01-20 .lt zone signed in test system.
- 2012-12-13 12:00 signed .lt zone, DS records from registrars are accepted.
- 2013-01-31 DNSSEC signing ceremony in KTU data center. .lt domain DNSSEC signatures were generated.
- 2013-02-20 DNSSEC in .lt enabled after IANA placed .lt domain DS records in root DNS servers.



# .LT DNSSEC CEREMONY





# PRIVATE DATA PROTECTION IN .LT



# PRIVATE DATA IN .LT

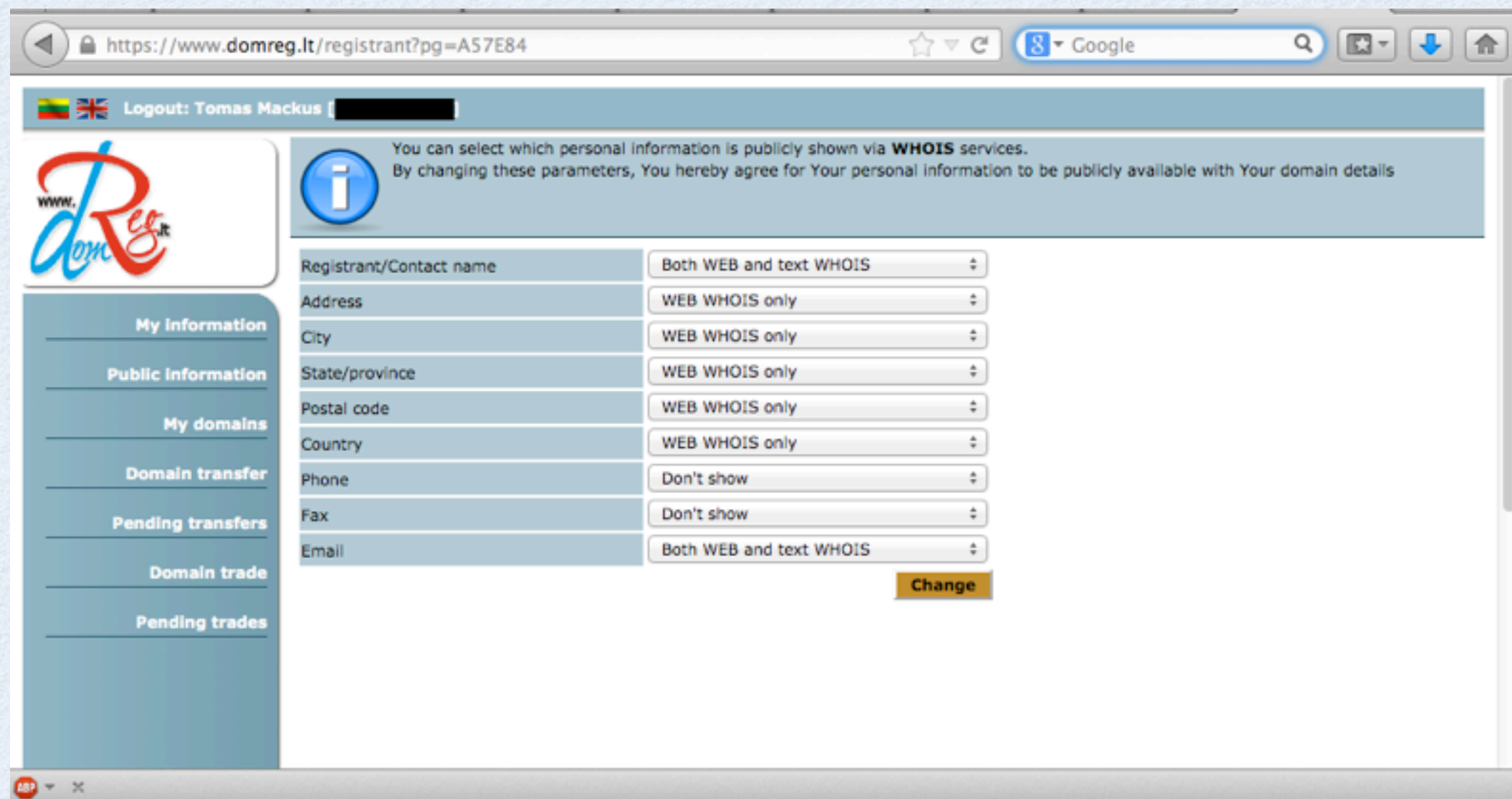
By default:

- If domain name registrant is private person, only his initials and contact e-mail address is visible in public web WHOIS database.
- Domain name registrant data is not shown via 43 port WHOIS database.



# PRIVATE DATA DISCLOSURE

Registrant himself can specify which of his personal data is shown publicly in WHOIS. This can be done via .LT domain registrant extranet.



The screenshot shows a web browser window with the URL <https://www.domreg.lt/registrant?pg=A57E84>. The page is for a user named Tomas Mackus. It features a sidebar with navigation links: My Information, Public Information, My domains, Domain transfer, Pending transfers, Domain trade, and Pending trades. The main content area has a header with a blue information icon and text: "You can select which personal information is publicly shown via **WHOIS** services. By changing these parameters, You hereby agree for Your personal information to be publicly available with Your domain details". Below this is a table of fields and their corresponding visibility settings.

Field	Visibility Setting
Registrant/Contact name	Both WEB and text WHOIS
Address	WEB WHOIS only
City	WEB WHOIS only
State/province	WEB WHOIS only
Postal code	WEB WHOIS only
Country	WEB WHOIS only
Phone	Don't show
Fax	Don't show
Email	Both WEB and text WHOIS

A "Change" button is located at the bottom right of the table.



THANK YOU!  
QUESTIONS ?