

Security Control Framework

“the World will only maybe need five computers!” - IBM’s Chairman, Thomas J. Watson, 1943

He may have been off by only two. That’s what Sun’s Chief Technology Officer Greg Papadopoulos predicts. The seven Global computers will be: Google, Yahoo!, eBay, Amazon, Microsoft, Salesforce.com, and the “Great Computer of China.”

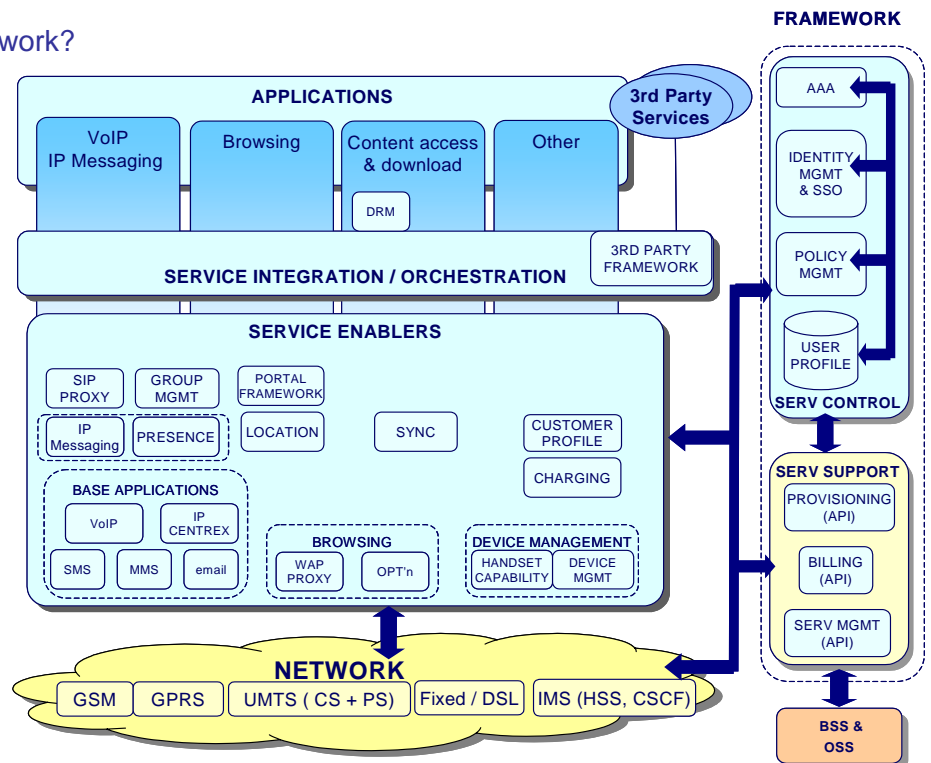
What is Security Control Framework?

Security Control Framework allows subscribers to use services and be protected based on intelligent policy management throughout a Telecoms Operator Infrastructure across all product lines. This is achieved by the Telecoms Operator Infrastructure being setup with a Telecom Services Architecture.

Telecom Services Architecture

Future telecommunications systems will be organized as a system of multiple, sometimes co-operating and sometimes competing, content providers and not as monolithic structures deployed by product line.

This is known as the Telecom Services Architecture:



Functional Areas

- ▶ Service Control via Security Control Framework with Intelligent Policy Management
- ▶ Service Support via Operational Support System
- ▶ Service Orchestration via Service Delivery Platform
- ▶ Applications via Value Added Services
- ▶ Service Enablers via Value Added Services

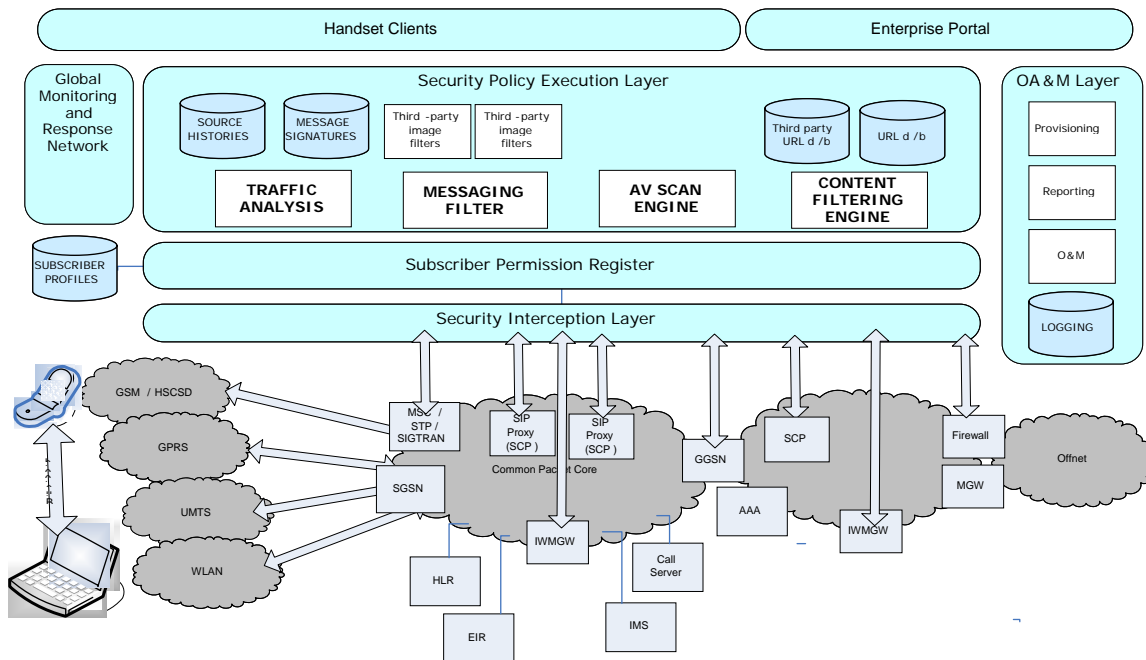
Key Requirements

- ▶ Applications with programmer efficiency
- ▶ Service Delivery Platform with multiple work streams
- ▶ Service Enablers with device efficiency
- ▶ Service Control with User profile for VAS details
- ▶ Architecture segments allows virtual Operations

Service Control Architecture

A key aspect of the Telecom Services Architecture is the Service Control Architecture for allowing access to services by subscribers through a Security Control Framework using Policy Enforcement and Decision Points within the Telecoms Services Architecture:

Security Control Framework



Responding to Network Attacks

Not only does the Security Control Framework allow subscriber use of Services, but it also provides protection against illegal or inappropriate content, mobile viruses and malware. It works across all Telecom Operator services (WAP, SMS, MMS, email, IM, ...), all forms of access (Fixed, Mobile, WiFi, WiMax) and for all media including internet, mobile internet, text, images, music, voice and video. This unified control provides protection and ensures the growth of data ARPU for mobile and convergent operators, and reduces churn through increased customer profiling. The Security Control Framework protects subscribers and network from malicious content within a Telecom Services Architecture.

Responding to Regulatory Pressures

The Security Control Framework is used by Telecoms Operators to respond to regulatory pressures, providing Parental Controls, Banning information on how to perform Terrorism, ... and extend corporate security policies.

Business Opportunity

The Security Control Framework will deliver:

- SMS Filtering - for interconnect and on-net spam and content controls;
- Subscription Management - for mobile content from service providers to subscribers
- MMS Filtering - for anti-viruses, anti-spam and inappropriate content.

- Email Filtering – for inbound and outbound mobile email messages to protect against transmission of viruses and spam.
- Corporate and Consumer Policy Management - to provide segment or customer-specific filtering policies.
- Mobile Web Filtering – for category and content based filtering of mobile web and WAP services.
- Malware and virus Filtering – a complete AV solution based on a two pronged strategy for defense against malware and virus threats to the network. The primary defense being provided by network based message filtering to detect and prevent viruses, and the secondary defense through delivering device and threat specific agents.
- Content analysis and advert insertion – providing the subscriber knowledge, policy controls and insertion engines to support mobile advertising and campaign management tools.
- Message Retention - Individual-specific controls on message retention policies.

The Security Control Framework delivers tangible value to the operator providing:

- Meeting regulatory requirements for parental and cultural controls;
- Subscriber-centric policy management across all bearers
- Revenue-generation through value-add consumer and corporate security services.