

Mobile Internet Enabling Proxy 4.0

Executive Summary

The Multi Service Proxy from Ericsson



Ericsson enables a smooth integration of the multimedia technology and business model into any existing mobile offering.

MIEP 4.0 is a true Multi Service Proxy, catering on its high Mobile Internet security!

All data and information contained in or disclosed by this document are confidential and proprietary information of Ericsson AB, and all rights therein are expressly reserved. By accepting this material, the recipient agrees that this material and the information contained therein are held in confidence and in trust and will not be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of Ericsson AB.

Information in this document is subject to change and does not represent a commitment on the part of Ericsson. Ericsson shall have no liability for any error or damages of any kind resulting from the use of this document.

All trademarks or registered trademarks are properties of their respective owners.

The Multi Service Proxy from Ericsson

Ericsson's Mobile Internet Enabling Proxy 4.0 is with its fourth release evolved to an advanced **Multi Service Proxy** – meaning a **One Vendor Solution** that can replace several proxies in the operators' network.

By simplifying the network an obvious OPEX reduction is achieved. By utilizing the features provided by MIEP, the operator will secure its portfolio of multimedia and content based services, and at the same time maximize its network performance.

MIEP is situated in the centre of the mobile Internet flow, and is crucial in mobile security offerings as well as in WAP and HTTP service offerings.

MIEP enable operators to offer:

- Fast and secure Internet Browsing
- Scanning for viruses in MMS messages, browsing content and downloads which ensures that the mobile device is protected from viruses and other malicious content
- Notification services
- Secure banking and download of games

MIEP 4.0 is designed to meet world-class scalability, performance, small physical footprint and operational efficiency for browsing traffic up to 10 000 transactions per second. This challenge puts high demands on the scalability.

MIEP is established on the market with more than 100 commercial customers, and has a proven track record with minimized unplanned downtime. The average availability for a MIEP system 2006 was 99,9966% (based on measurement for all live MIEP systems, both Single Node and High Available Scalable configurations).

Simplify your network for obvious OPEX reductions



The Ericsson Mobile Internet Enabling Proxy is a complete, one vendor solution offering seamless integration with core network through standard interfaces. For operators and service providers this means immediate cost reductions at the same time as their performance of service offerings and consumer security is maximized.

Service Optimization Will Increase Revenues



MIEP is the perfect enabler for providing services such as multimedia messaging, browsing, download and WAP push. To support these services, MIEP has extensive functionality for user access control and forwarding of user and network information to the service providers. This means that MIEP enables the web page layout and the content to be adapted to fit the small screen of the mobile terminal when browsing the Internet using a mobile device.

Comprehensive statistics for Pull and Push Services will give the operator the opportunity to optimize their service offerings according to user preferences.

MIEP enables operators to gain further revenue by attracting new users, increased retention and better offerings for associated service providers.

Boost Profit with Subscription Based Services



URL Filtering and Anti-Virus are features that the operator can provide to users as subscription based services.

MIEP's Mobile Internet security offerings are aimed for HTML and WML featured mobile phones. The security features included in MIEP are Anti-Virus, URL Filtering, user privacy towards content providers, and strict transport level security for services where money is involved, like gambling and banking.

Anti-Virus

The Anti-Virus feature protects mobile devices against harmful content, for example, executables such as Java downloads and MMS messages. MIEP forwards potential harmful content that need to be scanned to an Anti-Virus Scan-Engine over ICAP.

Scanning of MMS messages, browsing content and downloads ensures that the mobile device is protected from viruses and other malicious content. To optimize the browsing performance, the Anti-Virus solution is designed so that only potential harmful content is scanned. What content that is to be scanned is decided by the Anti-Virus module in MIEP, based on configurations done by the operator.

The Anti-Virus solution is fully configurable to provide flexibility for the operator. To optimize the browsing performance, the solution is designed so that only potential harmful content needs to be scanned, based on configurations done by the operator.

URL Filtering



URL Filtering is used to ensure that a user cannot access web pages that contain harmful information for the specific user group the user belongs to. Each subscriber is categorized into a user group, for example, Child, Adult, or Enterprise in the subscriber database. For each of the groups, the operator defines which content categories users of the group are denied access to.

URL Filtering is beneficial for parents who want to have control of the content that their children consume. Under aged can for example be protected from URLs belonging to gambling, adult content, and violence. URL Filtering can also be used for corporate subscriptions to reduce company cost for irrelevant and inappropriate surfing.

Customization Reduce Operational Costs

It is possible to customize the browsing proxy behavior by using URL rules and customized workflow scripts. Time-to-market for a customized MIEP behavior, new proxy services and new external interfaces is significantly shortened. It is also possible to temporarily fix device related bugs using device-specific pre-processing scripts. Some changes can be done by only editing a default workflow script or customizing a workflow script template. Other changes require the developing of a new proxy module. Many changes can be introduced without waiting for the next MIEP release.

Reduce CAPEX with Multi Operator Support

Multi Operator Support means that one physical node can handle mobile services traffic for up to 20 affiliate operators. The operator can provide proxy services to their affiliate operators and sell proxy services to small operators that do not need the full capacity of a MIEP node.

By using the Virtual Gateway feature, one MIEP node can handle Internet traffic from several networks - networks that may be geographically or business wise separated, and thus needs their own MIEP performance. For example, MIEP can use different subscriber identification and/or authentication mechanisms depending on if it serves a GSM or CDMA network. Operational costs will be reduced since an operator with affiliates only needs to buy one MIEP and place it in a central location.

MIEP can be configured to store CDR and statistics data specifically for each Virtual Gateway in separate files and folders. Affiliate operators can then fetch CDR and statistics information to their own billing and post processing systems.