Explicitly Authenticated Proxy

salvatore.loreto@ericsson.com

IETF 90 – July 2014
The goal
to define an intermediary to 'http' traffic, that is TLS connected to the browser, operates with the knowledge and explicit consent of the user.
A different proxy category

A good Proxy:

• Reduces data usage

• “Detects malicious pages and protects you from phishing, malware and harmful downloads”

• Does not interfere with access provided by your carrier, but may offer optional services
In a world where the client, intermediaries and server all embrace in a group hug, the user would get

a great user experience and end-to-end cryptography.
An Explicitly Authenticated Access Proxy will help network management functions (respecting RFC 7258)
An access network example

For a mobile network operator is important (MUST ensure) that the radio towers do not get so congested that data cannot be delivered, or is delivered with an unacceptable latency:

Web browsing, email, VoIP call, video call, streaming video, online gaming messages, chat content types have distinct needs regarding latency and bandwidth;
if the radio towers are able to detect and distinguish data content type they can be queued accordingly and without discrimination to customers or content providers
Regulatory mandate

Network operators are regulated by legal authority. This places them under obligation to restrict access to sites under a court order.
Explicitly Authenticated Proxy

BUILDING BLOCKS
Proxy Certificate

To help HTTP user agents identify and distinguish Explicitly Authenticated proxies from other servers (e.g. web servers), Explicitly Authenticated proxies should have a certification authority issued public key certificate.
Proxy Certificate

To help HTTP user agents identify and distinguish Explicitly Authenticated proxies from other servers (e.g. web servers), Explicitly Authenticated proxies should have a certification authority issued public key certificate.

Proxy Certificate does not make the Security UI more complex!
Opt Out mechanism

The user must consent to the proxy, and must be provided a mechanism to opt out from the proxy whenever they decide.

The UI to achieve this can be optimized (for example in the client settings rather than per-request interstitial pages).
Proxy request

Dynamic Logo

Choice

What does this certificate mean?

By accepting the proxy request you allow the proxy server to perform the following actions on your device:

Dynamic Services offered by MSP