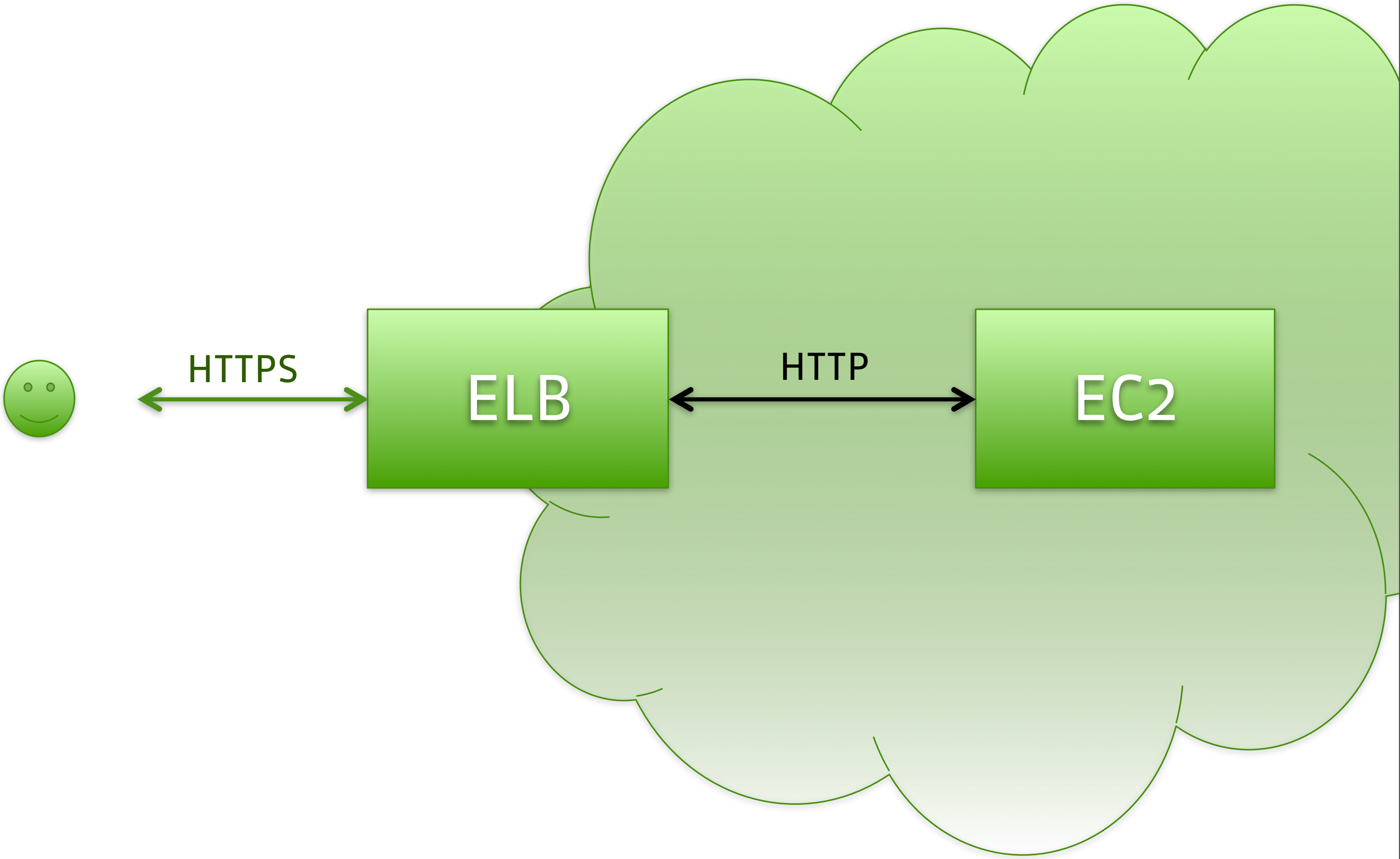
Futurice

Sovelluksen suojaaminen SSL:llä

Olli Ahonen

27.4.2011

1. SSL-TERMINOINTI ELB:SSÄ



1. SSL-TERMINOINTI ELB:SSÄ

```
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBANJdKoGXKLr00bcqyRaNSp67QoR2nUgGtCN79iwlxhzgMmATY8Ob
mDXR6TfDbMSa2cYgVFzDTvkCxThOHms4hJ8CAwEAAQJBAIGTQYtxQHVoN4VLpXFu
tnfvgJl3NooXFv6EbK3k1pMRp47IM6gKIiHzY96Q2TSLU41oYRxFsLD2voBR+QaG
UAECIQD2cSdFMPMyHNTQUFQIfDkvGVNXWTUy1xHqIZQYESZQgQIhANqFzffpoO1g
lsg5y8dHpHtWEpqP1xVkwpcpsqjy4kUfAiEAn+LjvoE2lyGbdJdZHbQyiXsd1gLb
f+OHDObCJScjO4ECIEWEhbbVozWBIdbG1DYsa341LqvvEJyktmcCg+zNgAA/AiEA
3OfB4ZsLT8Vc22tyJizHcD/U0nH5tEXbd4Ju9DCaoTA=
-----END RSA PRIVATE KEY-----
```

1. SSL-TERMINOINTI ELB:SSÄ

```
-----BEGIN CERTIFICATE-----
MIIDBTCCAq+gAwIBAgIJAMeAm94bxZh/MA0GCSqGSIb3DQEBBQUAMIGLMQswCQYD
VQQGEwJGSTEQMA4GA1UECBMHRmlubGFuZDEOMAwGA1UEBxMFVmFhc2ExFjAUBgNV
BAoTDUtvdGlwaXp6YSBPeWoxFjAUBgNVBAMTDUtvdGlwaXp6YSBFUlAxKjAoBgkq
hkiG9w0BCQEWG2tvdGlwaXp6YS1raXRhQGZ1dHVyaWNlLmNvbTAeFw0xMTAzMjgw
OTAzMDVaFw0xMjAzMjcwOTAzMDVaMIGLMQswCQYDVQQGEwJGSTEQMA4GA1UECBMH
RmlubGFuZDEOMAwGA1UEBxMFVmFhc2ExFjAUBgNVBAoTDUtvdGlwaXp6YSBPeWox
FjAUBgNVBAMTDUtvdGlwaXp6YSBFUlAxKjAoBgkqhkiG9w0BCQEWG2tvdGlwaXp6
YS1raXRhQGZ1dHVyaWNlLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDSXSqB
lyi69NG3KskWjUqeu0KEdp1IBrQje/YsJcYc4DJgE2PDm5g10ek3w2zEmtnGIFRc
w075AsU4Th5rOISfAgMBAAGjgfMwgfAwHQYDVR0OBBYEFDywpNQVxN69ozli4NfI
dw2zK3sYMIHABgNVHSMEgbgwgbWAFDywpNQVxN69ozli4NfIdw2zK3sYoYGRpIGO
MIGLMQswCQYDVQQGEwJGSTEQMA4GA1UECBMHRmlubGFuZDEOMAwGA1UEBxMFVmFh
c2ExFjAUBgNVBAoTDUtvdGlwaXp6YSBPeWoxFjAUBgNVBAMTDUtvdGlwaXp6YSBF
UlAxKjAoBgkqhkiG9w0BCQEWG2tvdGlwaXp6YS1raXRhQGZ1dHVyaWNlLmNvbYIJ
AMeAm94bxZh/MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADQQBAx3PFk4cu
xcDAk+55K2NFa3tz5Nz5sFW/Tn9IJrNKxjoV9KD8LgpSEq2qyBVzw74AIrF6D045
```

1. SSL-TERMINOINTI ELB:SSÄ

- X-Forwarded-Proto
- X-Forwarded-For

1. SSL-TERMINOINTI ELB:SSÄ

- X-Forwarded-Proto
- X-Forwarded-For

- XForwardedSupport=127.0.0.1,???

1. SSL-TERMINOINTI ELB:SSÄ

- X-Forwarded-Proto
- X-Forwarded-For

- XForwardedSupport=127.0.0.1,???

1. SSL-TERMINOINTI ELB:SSÄ

- X-Forwarded-Proto
- X-Forwarded-For

- XForwardedSupport=127.0.0.1,???

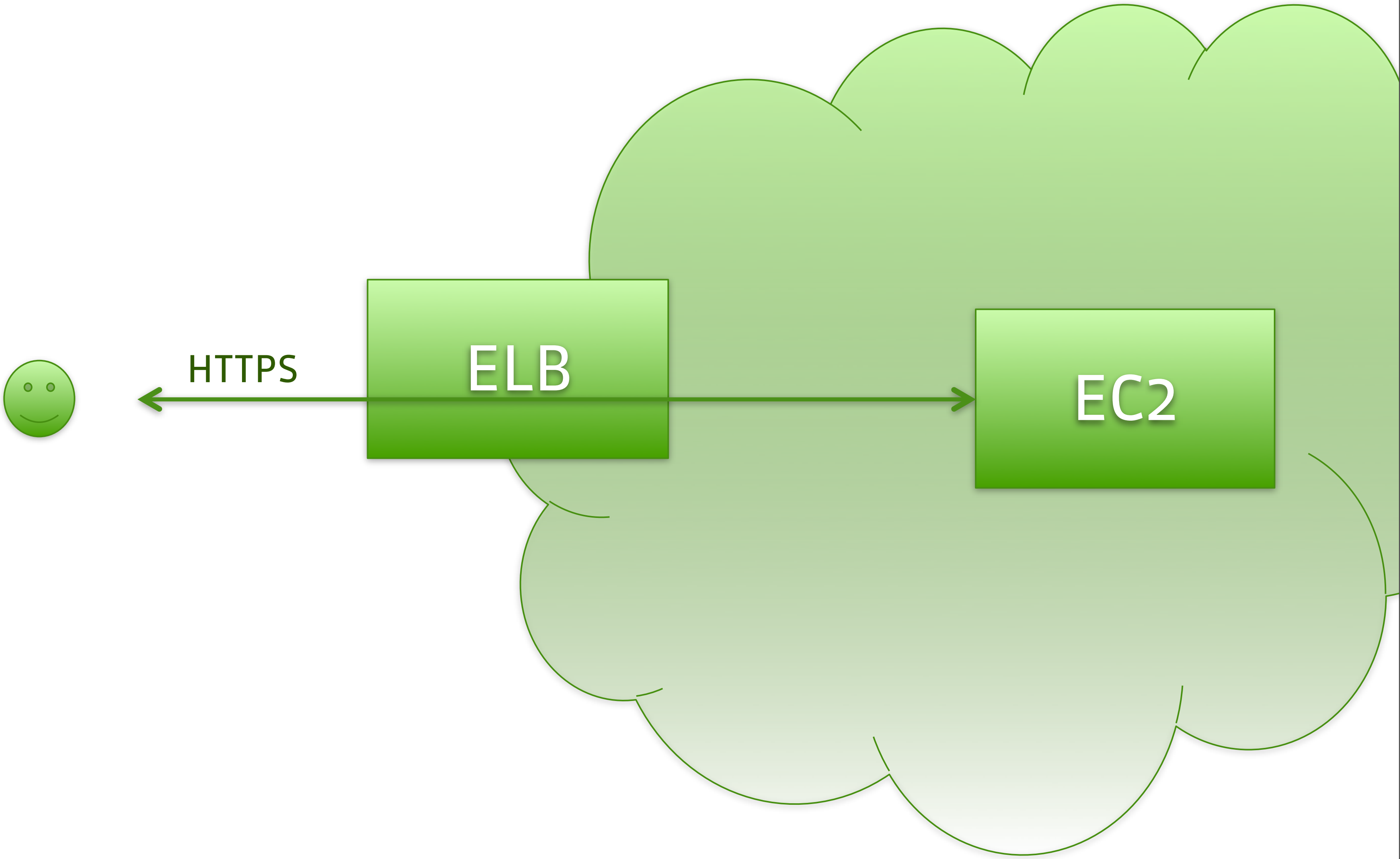
- https->http

1. SSL-TERMINOINTI ELB:SSÄ

```
public static Request parseRequest(ChannelHandlerContext ctx, HttpRequest nettyRequest)
throws Exception {
        //...

        if (Play.configuration.containsKey("XForwardedSupport")
        && nettyRequest.getHeader("X-Forwarded-For") != null) {
                if (!Arrays.asList(Play.configuration.getProperty("XForwardedSupport",
                                        "127.0.0.1").split(",")).contains(request.remoteAddress)) {
                        throw new RuntimeException("This proxy request is not authorized: " +
                                        request.remoteAddress);
                } else {
                        request.secure = ("https".equals(Play.configuration.get("XForwardedProto"))
                                || "https".equals(nettyRequest.getHeader("X-Forwarded-Proto"))
                                || "on".equals(nettyRequest.getHeader("X-Forwarded-Ssl")));
                        //...
```

2. SSL-TERMINOINTI EC2:SSA



2. SSL-TERMINOINTI EC2:SSA

- https.port=9443
- certificate.key.file=dev.key
- certificate.file=dev.cert

ASK ANYTHING