Web Weaving

Janvossensteeg 37
2312 WC Leiden
The Netherlands

# Compensating measures for insecure TSL on CDN

The (new) TEKs are to be distributed several times a day to all mobile phones participating. At a national scale this implies the use of a Content Delivery Network (CDN), best effort fetches and careful randomisation in case of failed fetches (to avoid a feedback loop & thundering herd synchronisation).

It is unlikely that a CDN at this scale can be build swiftly. It is also unlikely that a commercial CDN for such volumes is engineered with end-to-end security as a first priority. As it is in the very nature of a distributed CDN that can scale to engineer it such that there are no end-to-end processes; but to decouple to a maximum and introduce as much caching as possible.

Secondly, for reasons of commercial scale – almost all commercial and public CDN need to support older cryptographic protocols such as SSLv3 and TLS/1.0.

Both these two aspect (no end-to-end/caching and old protocols) trade integrity for scalability.

## Control needed

However the TEKs require reliable end-to-end delivery (i.e. no ability to be tampered with). As to not allow an adversary[1] to modify it in transit.

## Measure

For this reason - in *addition* to the HTTPS provided by the CDN - the TEKs distributed will be signed (or authenticated) by a pki-overheid certificate (in much the same manner as a pki-overheid certificate authenticates a webserver) at the origin. And the mobile application will verify this certificate against the pki-overheid root certificate (and chain) -and- against a build in ‘*pin*’ on that root.

[1] Or a script-kiddy who wants to *contaminate* her entire school.

## History

| | |
|---|---|
| 1.00 | First version (2020-06-22) |
| 1.01 | Added specific ref to SSLv3 and TLS/1.0 (2020-08-11) |

## About WebWeaving

WebWeaving has offered hands-on specialist consultancy and internet engineering. Since 1994 we have helped startups and large companies scale on the internet, drawing from a large network of technical experts. Scale not just in terms of hardware and bandwidth; but also scale in terms of staff and the organisational capability to continuously release and refine its products and software efficiently, timely and predictably. We help organisations understand the software life cycle and the total cost of ownership (including that of open source) relative to their ambitions.