7 November 2014 Study · Web & Cloud · Digital Identity

Analyzing HTTPS services offered by GV.AT domains

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/analyzing-https-services/

In this project several properties of the services offered by **gv.at** domains have been analyzed. The main emphasis of the analysis was placed on services that were offered via HTTPS (SSL, TLS protocols). The results of this analysis are presented in a technical report. In addition to the analysis, a basic framework for the automated analysis has been implemented.

The main results of the analysis are summarized as follows (note, that this is a snapshot taken in 2014. The distrubution meanwhile likely has changed):

- 1285 services have been analyzed, 763 of those services did not support HTTPS
- For the 552 services which offer HTTPS, the following details were observed:
- 59 services were configured for HTTPS. The other 463 services offered default HTTPS services (e.g. provider-specific default HTTPS certificates, or non-valid test certificates)
- The services have then been analyzed for their supported cipher-suites, which have a strong influence on the security of the TLS protocol.

All details are available in the project report (German only).

Use of SHA-1 in certificates

Multiple vendors of web browsers are intending to retire the popular hash algorithm SHA-1 in favour of more recent alternatives. Therefore, guidelines have been elaborated that plan to take a leave of SHA-1 in multiple steps.

The subsequent table illustrates the support for SHA-1 in a chronological manner and highlights the handling according to the browser (situation in 2014). The gradual sunset of SHA-1 is shown separated into steps whereas each is assigned an individual color: Notice (green), Warning (yellow) and escalation (red).

During the HTTPS analysis, a list of signature algorithms used on servers of public institutions, has been composed. Based on that, the following key figures can be derived (situation when completuing the study in 2014):

- 41 servers use a certificate which is no longer valid after 1/1/2016.
- 21 out of 91 certificates are still valid in 2016. Major browsers will consider the affected servers secure, with minor errors.
- 27 remaining certificates will be still valid after 1/1/2017. As a consequence, they will appear indifferent to unprotected HTTP connections, starting with the release of Google Chrome in version 40.

A detailed description of all deprecation policies and the list of investigated certificates are explained in project report (German only).