15 February 2016 Study · Privacy & Crypto · E-Government

Security Recommendations for the Public Sector

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 This content is no longer updated.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/security-recommendations-for-the-public-sector/

The application of cryptographic methods is a complex task. It requires the selection of appropriate methods that are able to meet given functional and security requirements. Furthermore, selected methods typically also need to be correctly parametrized, in order to achieve the intended security level. A well-known example is for instance the selection of suitable key sizes.

The complexity behind cryptographic methods and the need for an appropriate parametrization pose a serious challenge in practice and can lead to potential security flaws, as wrong algorithms or bad parametrizations can compromise the overall security. This also applies to frequently used cryptographic applications such as SSL/TLS, which rely on cryptographic primitives like authentication, encryption, or integrity checks.

Being aware of these issues, A-SIT has prepared two studies, in which recommendations regarding the proper selection of cryptographic algorithms, their application, and their parametrization are provided. The first study focuses on cryptographic primitives and identifies those algorithms, which are recommendable for achieving data integrity, confidentiality, and authenticity. In addition, appropriate parametrizations for these algorithms are recommended where required. Special focus is put on those aspects and scenarios, which are of special relevance in the Austrian public sector. The second study focuses on the correct application of SSL/TLS. Several general recommendations are provided and appropriate cipher suites are recommended.

Even though both studies are primarily addressed to public administrations, the contents of these studies are potentially also interesting for private-sector companies and organizations, or for end users. Therefore, these studies are provided as free download on this website.