Information security requirements

This chapter describes the requirements that apply to the information security measures that are implemented.

- Digital signature
- DNSSEC
- Encryption
    - SAML encryption — Encryption in combination with SAML is achieved via XML-encryption. This paragraph provides an explanation of encrypted elements as well as elements encrypted to multiple recipients.
- End-to-end encryption — End-to-end encryption is applied in Elektronische Toegangsdiensten to protect user privacy. This in order to avoid an Herkenningsmakelaar (HM) becoming an unintended hotspot for information on service usage. Below is an explanation of how end-to-end encryption works out across various interfaces.
- Native apps — It is permitted for roles in the network to expose their functionality as a native mobile app, instead of a (responsive) website. This section descibes the conditions which apply, and the desired message flows.
- PKIoverheid
- Secure connection
- Secure cookies
- Synchronize system clocks