13 August 2014 Study · Digital Identity · Mobile Security

Alternative Two-Factor Authentication

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 This content is no longer updated.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/alternative-two-factor-authentication/

Two-factor authentication (2FA) is an essential mechanism that enables secure access to remote services. The Austrian Citizen Card is only on example of many solutions that rely on the concept of 2FA. Most 2FA methods have been designed and developed for classical end-user devices such as desktop PCs and laptops. Examples are smart card based solutions or the SMS–TAN approach. During the past years, mobile end-user devices have significantly gained importance. As these devices differ from classical end-user devices in terms of handling, security features, and functionality, established 2FA methods can often not be applied on these devices.

As a first step towards a solution to this issue, A-SIT has systematically analyzed and assessed different approaches to securely implement 2FA methods on current mobile end-user devices. Results of these analyses and assessments have been collected in a survey. This survey basically covers the following aspects:

- The survey provides a brief overview of underlying concepts of 2FA.
- It identifies requirements of 2FA methods for mobile end-user devices by means of an abstract model.
- Existing 2FA approaches are assessed against the identified requirements.
- Obtained assessment results are used to develop a solution.
- The applicability of the solution is evaluated by applying it to the concrete use case of server-based signature solutions.
- The feasibility of the developed solution is assessed by means of a prototype implementation.

In summary, the survey shows that mobile end-user devices offer various opportunities to implement alternative 2FA methods. Furthermore, the survey shows that these methods can be integrated into existing applications, in order to ensure their security and to prepare them for access by mobile end-user devices.