

INSIKA Status Report November 2015

Current as of: 9 November 2015

INSIKA (acronym for “INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme” meaning “integrated security solution for cash registers processing metered values”) is a method that is open to all types of technology and aims at securing the digital accounting records of cash transactions by using electronic signatures. It can be used for cash registers, taximeters and similar devices.

Based on the stable technical standard a number of functioning implementations is available. In taximeters, INSIKA is successfully applied on a large scale. Several manufacturers of cash registers implemented INSIKA and tested it successfully in practice; however, no legal certainty can be obtained for the time being for lack of a legal basis.

INSIKA is future-proof. Adjustments to additional technical requirements and higher cryptographic safety standards have already been made or are being made. There is a worldwide interest in the INSIKA method, documentation and test smart cards. In Austria, INSIKA served as template for the safety regulations for cash registers.

After the legal introduction failed in 2008, INSIKA has been subject of the political discussion in Germany again since April 2014. Despite an increased demand for legal introduction of INSIKA in Germany, this process has so far failed to produce results.

INSIKA and ADM e.V.

From 2008 to 2012, the Physikalisch-Technische Bundesanstalt (the National Metrology Institute of Germany) together with industrial partners developed and tested INSIKA based on the concept of the German fiscal authorities. Since the project was completed successfully, the concept and its resulting technical procedures have been supported and further developed by the ADM e.V. (German User Association of Decentralised Measurement Systems).

The INSIKA method can be used without patents, licence costs or similar constraints. The ADM e.V. does therefore not pursue any commercial interests. The members' main objective is rather to establish a safe, inexpensive and easy-to-use method to secure the electronic accounting records of cash transactions, in order to provide a true alternative to the complex and costly certification procedures of conventional “fiscal POS systems”. A special focus is on legal certainty for the users.

Method stable and available for years

The INSIKA method has been a stable standard since 2010. At present, profiles for cash registers and taximeters are available. The profiles define the mapping of the respective, application-specific data.

A smart card is presently used as security anchor, which is indispensable for high-security systems. Sample cards for interested manufacturers have been available since 2010. The D-Trust GmbH (a 100% subsidiary of Bundesdruckerei GmbH / Federal Printing Office) produces cards for live operation in taxis.

Mass-production devices available and used in practice

Today, all renowned producers of taximeters offer security units with integrated INSIKA card on the German market. Nearly 5% of all German taxis are already equipped with taximeters, which deliver signed recordings according to the INSIKA method. Data is sent via a standardized, open interface to a data server. The taxi operator can select one of several competing providers.

Cash registers do not have a control unit comparable to the taximeter and there is no market surveillance similar to the public traffic authorities. For these reasons, the appropriate application of cash registers with INSIKA would require binding legal regulations to ensure the acceptance of signed data. Nevertheless, nine manufacturers of cash registers have already developed operational systems. INSIKA has undergone field tests; some have been running for several years.

The implementation costs that were estimated in the course of the project have been confirmed by

companies which integrated INSIKA to their systems.¹

Future-proof

INSIKA was designed in such a way that adjustments to new security and technical requirements can easily be made. The adjustments for taximeters for instance could be realized without changing the method.

Several further developments are in progress:

- The use of a new smart card generation is being prepared
- Optional use of ECDSA-256 signatures instead of ECDSA-192 to support the currently recommended key lengths
- New export format for cash registers to simplify audits and to improve processing speed
- New profiles for additional applications

Worldwide interest

INSIKA is known worldwide. So far, more than 500 companies, institutions, authorities or individuals from 34 countries have retrieved the INSIKA specifications; almost 300 test cards have been issued (212 were ordered and approx. 70 were provided separately for test purposes).²

Country	Retrievals	Cards
Germany	296	142
Austria	143	36
Netherlands	10	7
Spain	6	6
Belgium	5	2
Bulgaria	5	2
Serbia	4	
France	4	2
Switzerland	4	
Sweden	3	3
Poland	3	2
Slovakia	3	
Italy	3	
21 other countries	27	10
Total	516	212

The INSIKA specifications have been available in German since 2010 and in English since 2014. In addition to the technical documentation and various technical articles, demonstration software and verification tools are available for developers, users and auditors.

INSIKA became template for security solution in Austria

On 1 January 2017 new safety regulations for cash registers will become effective in Austria. They require that every cash register is equipped with a safety mechanism based of electronic signatures and smart cards. All the essential basic ideas were adopted from INSIKA. However, numerous details were changed for political reasons.³

Status in Germany

For about one and a half years now, the political discussions about a legal introduction of the INSIKA method have been resumed. It is not the task of the ADM e.V. to comment this. However, as numerous misunderstandings and misinformation circulate in the discussion, the ADM e.V. published various papers about the most important issues.⁴

Manufacturers of cash registers and industry associations campaign for the compulsory introduction of the INSIKA method. They have recognized that this approach allows obtaining legal certainty and provides the best possible cost-benefit ratio.

In contrast, software and hardware certification of cash registers, taximeters etc. would be considerably more expensive and detrimental to innovation. For reasons of cost alone, the indispensable, permanent conformity check of all installed devices is impossible.

Contact

INSIKA – ADM e.V.
An der Corvinuskirche 22-26
D-31515 Wunstorf

www.insika.de
E-Mail: info@insika.de

¹ http://public.ptb.de/oa/doi/210_20130206e.pdf (in German)

² Current as of 4 November 2015

³ Changes of the method lead to losses in terms of security and fault tolerance. Analysis of the ADM e.V. (in German): http://www.insika.de/images/stories/INSIKA/Analyse_RKSV_oesterreich.pdf

⁴ Available (in German) at: <http://www.insika.de/de/letzte-neuigkeiten>