Position Paper

Position Paper on the EPC Sercurity Requirements for Remote Payments

2013-08-06

The Federal Association for Information Technology, Telecommunications and New Media (BITKOM) represents more than 2,000 companies in Germany. Its 1,200 direct members generate an annual sales volume of 140 billion Euros annually and employ 700,000 people. They include providers of software and IT services, telecommunications and Internet services, manufacturers of hardware and consumer electronics, and digital media businesses. BITKOM campaigns in particular for new convergent industry solutions, the modernization of the education system, for an innovative economic policy and a future-oriented Internet policy.

In the last couple of years the requirements for digital payments have changed dramatically. The use of remote or mobile payment solutions have been widely used and accepted. From payments via NFC or QR code to new systems that offer credit card payments via smartphone – today there are numerous different possibilities to pay digital.

Innovations and customer oriented individualized value added services will be the incitement of future remote payment solutions. Those new solutions give room for new business models and customer services not only for the new entrants but especially for banks.

BITKOM welcomes the EPCs engagement on secure solutions in the best customer interest. We believe that security is an important part in the user acceptance process, but some of the recommended requirements in the Annex 4 are to one sided and hinder the further broadening of remote payments.

BITKOM suggests the following:

- Line 367, Req S2: It is not clear if a basic e- and m-commerce transaction requires static or strong authentication, due to 6).

- Line 371, Req S4: ISO 9564 and PCI PIN requirements were developed for card transactions, and are difficult to implement for remote payments transactions.

- Chapter 4.2.3.2.: There are many security requirements mentioned which are not very clear. Fulfilling requirements like DP1 “secure environment are protected against unauthorized disclosure” or DP3 “cryptographic services shall be protected from exploitation” can never be fulfilled 100%. Recommended countermeasures need to be specified in more detail.

- The security requirements for strong authentication and secured e- and m-commerce transaction can only be fully met by either fulfilling hardware requirements which are not available for mobile handsets today (TEE) or which are extremely inconvenient to use for the end user for

Federal Association
for Information Technology,
Telecommunications and
New Media

Albrechtstr. 10 A
10117 Berlin-Mitte
Germany
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Contact
Steffen von Blumröder
Head of Banking & Financial Services
Tel.: +49.30.27576-126
Fax: +49.30.27576-51-126
s.vonblumroeder@bitkom.org

President
Prof. Dieter Kempf

Management
Dr. Bernhard Rohleder

mobile use cases (external security tokens). We are afraid that payment methods fulfilling these high security standards will have (too?) high barriers for user acceptance. Therefore making it impossible to establish remote payments for mobile in the market.

- We highly recommend to define a standard for different levels of security for remote payments transactions explaining potential risks of a transaction so that it is understood by the end user. So that end users can better evaluate and decide which level of security and convenience they want to apply for their transactions.

We would appreciate an involvement in the further discussion to foster a mutual agreement in the definition of new rules between banks on the one hand and the digital economy on the other hand that BITKOM represents.