EUROPEAN FORUM
ON THE SECURITY OF RETAIL PAYMENTS

ECB-PUBLIC

30 April 2013

# TEMPLATE:
# COMMENTS ON THE DRAFT "RECOMMENDATIONS FOR PAYMENT ACCOUNT ACCESS SERVICES"

| | | |
|---|---|---|
| **Contact details (will not be published)** | Mr | Martin Stein<br><br>Deutscher Sparkassen- und Giroverband, Charlottenstraße 47, 10117 Berlin<br>on behalf of<br>German Banking Industry Committee (GBIC) |
| | martin.stein@dsgv.de | |
| | +49 30 20225-5515 | |
| ☐ | The comments provided should NOT be published | |

The table below shall serve as a template collecting comments received in a standardised way.

- Please **add** to the table **only issues where you consider that a follow-up is necessary**, i.e. no general statements like "We welcome the recommendations."
- All comments should be **separated per issue** concerned so that a thematic sorting can be easily applied later on. (i.e. one row for each issue).
- If needed, replicate page 2 for the provision of further comments.

The assessment form consists the four items which are suggested to be filled as follows:

- **Originator:** Name of the originator and ISO code of the country of the originator (e.g. NAME (AT/BE/BG/...))
- **Issue** (states the topic concerned): General comment, Scope, Terminology, REC 2, 1.1 KC, 3.2 BP, Glossary,
- **Comment:** Suggestion for amendment, clarification or deletion
- **Reasoning:** Short statement why the comment should be taken on board

**Originator:**

| | | | |
|---|---|---|---|
| **Name of the originator (e.g. name of the company or association)** | German Banking Industry Committee (GBIC) | ISO code of the country of the originator | DE |

**Comments on the recommendations for "payment account access" services**

| Issue | Comment | Reasoning |
|---|---|---|
| **General comments** | Amendment; Clarification | The goal to define regulations for account access services is generally supported. It is important that competitors of PSPs, which are currently not covered by the recommendations for the security of internet payments are subject to the same security considerations like PSPs itself.<br><br>However there are some general considerations:<br><br>The recommendations only cover a specific account access scenario, where a Third Party Service Provider (TP) authenticates himself with respect to the PSP using either the TP's or the customer's credentials – and gets full access to the user's account. Especially in case of payment initiation services, other scenarios are conceivable, where most of the problems concerning protection of sensitive payment data will not occur.<br><br>For instance whilst executing the payment, the user could be redirected to its online banking account, where he enters its secret authentication credentials in a secure environment. This scenario is used in several online payment schemes across Europe. This procedure provides advantages especially concerning data security and data privacy. It should be amended that where applicable the general account access scenario should be replaced by such specific solutions. At least the two main scenarios "account information service" and "payment initiation service" should be distinguished. Different recommendations should be given depending on the specific scenario.<br><br>Whereas in case of payment initiation services, data protection can be ensured by specific solutions, in case of account information services data protection remains a crucial issue. Therefore it has to be |

| | | |
|---|---|---|
| | | ensured that neither European nor national data protection law will be violated by those services.<br><br>Another more technical scenario is the communication via a banking protocol offered by PSPs. Banks at least in Germany offer a banking interface which can be accessed by banking software products. Common web interface communication is dedicated to personal access by users only and not for third parties. Existing banking interfaces however offer common procedures for identifying consumers and third parties and are able to restrict the access only to the banking transactions necessarily required by the TP.<br><br>Furthermore a general clause is missing describing the consequences of violation and misuse of the recommendations. Regarding the relationship between TP and PSP, misuse should give PSPs the right to cancel any contractual agreements. |
| **Recommendation 1:** Governance | | In order to achieve identical requirements for PSPs and TPs the recommendations are appreciated. A concretisation might be wishful by referring to internationally agreed security standards like ISO/IEC 27001. |
| **Recommendation 2:** Risk assessment | | In order to achieve identical requirements for PSPs and TPs the recommendations are appreciated. |
| **Recommendation 3:** Incident monitoring and reporting | | In order to achieve identical requirements for PSPs and TPs the recommendations are appreciated. |
| **Recommendation 4:** Risk control and mitigation | | In order to achieve identical requirements for PSPs and TPs the recommendations are appreciated. |
| **Recommendation 5:** Traceability | Amendment; Clarification | 5.6 KC: The requirement that PSPs should be able to differentiate between payment account access by TP and payment access by customers is not feasible, in case the TP uses the user's credentials for identifying himself. The distinction between different users will be achieved by different authentication credentials. In case of TPs using the user's credentials a distinction is not possible. Instead of recommendation 5.6 KC it should be therefore required that TPs have to identify themselves with respect to the PSP. Because third party identification is commonly not supported by web banking applications other means should be used. In case of payment initiation services bilaterally agreed |

| | | |
|---|---|---|
| | | purpose codes could be defined and contractually agreed.<br><br>Best practice 5.1 which recommends to provide customers with specific credentials to be used for account access services only would solve this issue, but generates costs especially for the PSP. Recommendation 7 - which promotes strong authentication - forces PSPs to issue secure tokens like smart cards or to use separate devices like mobile phones. Issuing a second secure token would confuse customers on one hand and on the other hand results in unaffordable costs, which must be carried by PSPs. |
| **Recommendation 6:** Initial Customer Identification and Information | | In order to achieve identical requirements for PSPs and TPs the recommendations are appreciated. |
| **Recommendation 7:** Strong Customer Authentication | Amendment; Clarification | The demand for strong authentication not only in the sphere of PSPs but also in the TP's sphere will be highly supported. It is important that competitors of PSPs, which are not covered by the recommendations for the security of internet payments are subject to the same security considerations like PSPs itself.<br><br>However it should be distinguished between scenarios where TPs issue their own credentials and tokens for strong customer authentication and scenarios where TPs use the strong authentication credentials issued by the PSP. In the latter case the definition of "strong authentication" presented is not applicable for account access scenarios, because the requirement "something only the user knows" does not comprise the case that not only the user but also the TP knows the secret credentials.<br><br>Therefore unfortunately the recommendations presented are in most cases not applicable for TPs, because authentication means and tokens are usually issued by PSPs. Most business cases of account access services rely on using the authentication details and tokens issued by the PSP. Therefore TPs are usually not forced to issue separate authentication measures on their own.<br><br>7.1 KC: An agreement between TP and account- servicing PSP to rely on the account servicing, PSP's authentication methods should strongly be supported. It should be amended that this agreement has to be mandatory and contractually fixed. |
| **Recommendation 8:** | | |

| | | |
|---|---|---|
| Enrolment for and provision of authentication tools and/or software delivered to the customer | | |
| **Recommendation 9:** Log-in attempts, session time out, validity of authentication | | Unfortunately the recommendations are in most cases not applicable for TPs, because the login process and the session timeout are usually controlled by the PSP. |
| **Recommendation 10:** Monitoring | | 10.2 KC: It is assumed that TP act on the basis of a contract with the merchant. Over that, there is a need for a contractual basis in the relation between PSP and TP for several reasons:<br><br>The TP uses the PSPs infrastructure and databases. It is a general legal principle that the use of external resources and intellectual property needs a contractual basis. This contract has to govern<br>• the rights of both the PSP and the TP<br>• identification of the TP (as the PSP has to know and to be able to tell the PSU who had access to the account)<br>• liability issues (as the TP should be liable to the PSP for any damage that is caused by the TPs service)<br>• cost allocation (as every transaction done by the TP raises the IT-costs of the PSP)<br>• security aspects (as the PSP can only guarantee a certain level of security to the PSU if is ensured that everybody who has access to the account is contractually obliged to provide the same level of security) |
| **Recommendation 11:** Protection of sensitive payment data | Amendment; Clarification | The definition of the term “sensitive payment data” in the glossary includes payment data as well as authentication data. We strongly recommend to distinguish between different classes of sensitive payment data, especially payment transaction data and user authentication data. Whilst payment transaction data are usually known also by the merchant, authentication data should remain in the PSP sphere. Concerning online banking in Germany, the terms of service demand the customer to keep his authentication data secret. In case of violation of these terms the user is responsible for misuse.<br><br>A further recommendation should be: TPs should be restricted to execute only those business |

| | | |
|---|---|---|
| | | transactions essentially necessary for the specific payment account access service. For example, payment initiation services should only be allowed to initiate payments and not to access stock accounts. On the other hand account information services should not be allowed to initiate payments. If these restrictions cannot be technically controlled, they should be contractually agreed between TP and PSP. Violation of these restrictions should give PSPs the right to cancel any contractual agreement.<br><br>It is not expressed that technical solutions could help to mitigate concerns regarding protection of sensitive payment data. For instance entering user credentials into a Java applet causes that the TP doesn't come into contact with this sensitive data.<br><br>11.6 KC: The recommendation that TPs should not use the account information for other purposes than those actively requested by the account owner is essential. It should be amended that in case of misuse PSPs should be entitled to cancel any contractual agreements. |
| **Recommendation 12:** Customer education and communication | | In order to achieve identical requirements for PSPs and TPs the recommendations are appreciated. |
| **Recommendation 13:** Notifications, setting of limits | | In order to achieve identical requirements for PSPs and TPs the recommendations are appreciated. |
| **Recommendation 14:** Customer access to information on the status of payment initiation | | In order to achieve identical requirements for PSPs and TPs the recommendations are appreciated. |