EBA STRONG AUTHENTICATION REQUIREMENTS

FOR INTERNET PAYMENTS IN EU TO BE IMPLEMENTED BY AUGUST 1ST 2015

LEGAL WHITEPAPER

What are the strong authentication requirements under EBA Guidelines which European banks are expected to comply to by August 1st 2015, and which technologies will not meet the requirements?

DEFINITIONS

- **EBA** European Banking Authority, is the European banking supervisory authority, established through Article 16 of Regulation (EU) No 1093/2010
- **ECB** European Central Bank
- **PSP** Payment Service Provider, defined as anyone covered by the requirements set out in Payment Services Directive [2007/64/EC]
- **OTP** One-time password.
- **2FA** Two factor authentication, defined in EBA guidelines as a procedure based on the use of two or more of the following elements - categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. static password, code, personal identification number; ii) something only the user possesses, e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint.

VERISEC

TABLE OF CONTENTS

1. Abstract 3
2. Status of EBA guidelines 4
3. Scope of the guidelines 4
4. Strong authentication requirements 5
5. Summary 7
6. Conclusion 7
7. Sources 7

ABSTRACT

This paper studies the EBA guidelines for strong authentication for payment services. These represent a “minimum requirements” standard for security of Internet payment services and they are a development of ECB recommendations and the underlying EU Payment Services Directive.

EBA guidelines clearly establish strong authentication requirements while remaining technology neutral (eg smart cards, OTP generators).

The guidelines define strong authentication as multi-factor authentication, in other words a procedure based on the use of several elements (at least two) in combination, categorized as knowledge, ownership and inherence. This is the same principle that underlies ATM security where the credit card is an “ownership” element and the PIN code is a “knowledge” element.

In addition to the multi-factor requirement, the guidelines also set additional requirements which will be analyzed in further detail in this paper. In summary they disqualify a number of technologies, eg simple OTP (i.e. not 2FA), grid cards solutions and technologies which do not encrypt the authentication data itself, eg, SMS OTP, i.e. where one-time passwords are sent to the user via SMS. They also disqualify technologies like TAN lsts where PIN codes or OTPs have a long validity period, and any solution where the OTP can be replicated or stored on a vulnerable media and stolen via the Internet.

> “PROVIDERS IN THE EU WILL BE EXPECTED TO IMPLEMENT BY 1ST AUGUST 2015”
>
> *EBA December 19th 2014*

STATUS OF EBA GUIDELINES

While the term "guideline" may seem to indicate non mandatory "best practices", it is clear from article 16(3) of EU Regulation 1093/2010 ("EBA Regulation") that competent authorities and financial institutions must make every effort to comply with them. The EBA expects all competent authorities and financial institutions to whom guidelines are addressed to comply with them.

According to the article above, competent authorities must also notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, within two months of the translations of the final guidelines being published.

Where the competent authority has not complied with Union law the Commission may, after having been informed by the Authority, or on its own initiative, issue a formal opinion requiring the competent authority to take the action necessary to comply with Union law. If this happens, the competent authority shall, within 10 working days of receipt of the formal opinion referred to in paragraph 4, inform the Commission and the Authority of the steps it has taken or intends to take to comply with that formal opinion

SCOPE OF THE GUIDELINES

The guidelines are to be read as minimum recommendations. Industry best practices and ECB recommendations can be both more onerous and detailed. It is still up to each provider of payment services authority to PSPs to monitor and assess the risks involved in their payment operations, develop their own detailed security policies and implement adequate security, contingency, incident management and business continuity measures.

The guidelines affect the following payment services:

Cards – The execution of card payments on the internet, including virtual card payments, as well as the registration of card payment data for use in 'wallet solutions';

Credit transfers – The execution of credit transfers (CTs) on the internet;

E Mandate – The issuance and amendment of direct debit electronic mandates;

E money – Transfers of electronic money between two e-money accounts via the internet.

> "LATEST PAN-EU FIGURES SHOWED THAT FRAUD ON CARD INTERNET PAYMENTS ALONE CAUSED €794 MILLION OF LOSSES IN 2012"

EBA December 19th 2014

Services which are excluded from the guidelines are:

- Other internet services provided by a PSP via its payment website (e.g. e- brokerage, online contracts);
- Payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology;
- Mobile payments other than browser-based payments
- CTs where a third party accesses the customer's payment account;
- Payment transactions made by an enterprise via dedicated networks;
- Card payments using anonymous and non-rechargeable physical or virtual pre- paid cards where there is no ongoing relationship between the issuer and the cardholder;
- Clearing and settlement of payment transactions.

Special cases with lower authentication requirements

According to the guidelines, PSPs could consider adopting alternative customer authentication measures for:

- Outgoing payments to trusted beneficiaries included in previously established white lists for that customer;
- Transactions between two accounts of the same customer held at the same PSP;
- Transfers within the same PSP justified by a transaction risk analysis;
- Low-value payments, as referred to in the PSD.

The reason for these exceptions is obviously that these transactions are deemed to be low risk and therefore do not warrant the same strong authentication requirements. This paper does not cover the requirements for these types of transactions.

STRONG AUTHENTICATION REQUIREMENTS

The EBA guidelines I-12 define Strong authentication against the following criteria:

"a procedure based on the use of **two or more of the following elements – categorised as knowledge, ownership and inherence:** i) something only the user knows, e.g. static password, code, personal identification number; ii) something only the user possesses, e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint.

In addition, the elements selected must be **mutually independent**, i.e. the breach of one does not compromise the other(s).

At least one of the elements should be **non-reusable and non-replicable** (except for inherence), and not capable of being **surreptitiously stolen via the internet**.

The strong authentication procedure should be designed in such a way as to **protect the confidentiality of the authentication data**."

Also section II-9 says that: "When using a one-time password (OTP) for authentication purposes, PSPs should ensure that the validity period of such passwords is **limited to the strict minimum** necessary. "

Analysis

The **first** requirement clearly mandates the use of two (or more) factor authentication. This is important because already, solutions relying on simple OTP:s without a second factor are not considered adequate. Many solutions, relying on just OTP tokens, or tan lists, would be disqualified.

The **second** point qualifies the 2FA requirement by saying that the factors need to be mutually independent. A breach of one of the factors should not compromise the other. In other words, if a mobile device is vulnerable in such a way that that both a mobile OTP app on a phone and a locally stored PIN code for logging into the device can both be hacked (a locally stored PIN can always be attacked using brute force), then the solution would fail this second requirement.

METHODS MEETING THE NEW GUIDELINES

Mobile with server stored PIN + app shield + encrypted data

Hardware tokens

Card readers

METHODS TO BE AVOIDED

Mobile with locally stored PIN

SMS

E-mail

Tan lists

Grid cards

Browser based OTP

The same is true if the OTP generator is a snap-in to the browser and the second factor is a PIN code that the user types in via the browser. Malware could take control of the OTP generator and a key logger could store the user's PIN code. This would not be an acceptable solution.

The **third** requirement states that at least one of the factors should be non re-usable and non-replicable, nor capable of being surreptitiously stolen from the Internet. This requirement would seem to apply primarily to the ownership factor, e.g. an OTP generator/ token, or similar, because knowledge and inherence are normally re-used. While most OTP solutions, even printed tan lists, could in theory meet the requirement, there are a number of solutions that don't.

A tan list stored or sent across the Internet would not do (and of course, a printed tan list can be scanned by the user and stored in a vulnerable environment). Neither would a grid card, because although the challenge will be different every time, a hacker able to log historic transactions will eventually learn all the positions on the grid. Such a system would fail the re-usability test.

The **fourth** requirement is that the authentication data itself is protected. Normally this requirement is satisfied using SSL encryption between the browser and the bank application. This is arguably not good enough though, because malware on a computer could record PIN codes and OTPs. Certainly, a solution based on OTP sent via unencrypted SMS, would not meet the requirement.

The **fifth** and final requirement, which relates to the validity of authentication, says that the validity of OTPs should be limited to the strict minimum necessary. The obvious case is a bank treating OTPs as "limited time" passwords, i.e. they can be used to gain access for a month. A less obvious case relates to tan lists, i.e. pre-printed lists of OTP:s. One problem with these lists is that people can duplicate them by taking pictures of them or copying/ scanning them, and storing them on various storage media including network connected phones and computers. Thus they would fail the test above, i.e. that the the element shall be "non-replicable".

Furthermore, with tan lists, the OTPs on the lists are valid until they have been used to authenticate with, which can be months and years. It therefore seems difficult to argue that tan lists could ever meet the requirement for an OTP limited to the minimum time necessary.

SUMMARY

The analysis above shows that some authentication in common use by banks across Europe simply cannot qualify as strong authentication based on the "tests" set out in the EBA guidelines.

Simple OTP generators with no second factor would not do. Neither would solutions where a breach of a PC or a mobile phone could compromise both factors. Examples are OTP apps with locally stored and validated PIN codes, as well as browser based OTP generators with PINs entered by the user into the browser.

It would also seem that SMS OTP fails the test of authentication data confidentiality and grid cards which re-use grid positions fail the non-reusability and non-replicability tests.

Likewise, a tan list which allows for OTPs to be replicated and stored in vulnerable places as well as being valid for a long time (i.e. until used) would fail the tests of "non-replicability" and "minimum necessary validity time".

CONCLUSION

The EBA guidelines require a strong authentication solution to be multi-factor, but no factor must be compromised due to the breach of another.

In the case of a mobile authentication device for example, PINs should not be stored locally because they could be subject to a brute force attack. Instead, PIN validation should be done server side. Also, the mobile device would require strong app shielding in order for key loggers to fail to log key-strokes and to take screenshots.

In the case of web based authentication, a separate hardware authentication device or a separate channel of authentication using a mobile phone app would be an appropriate solution.

Grid cards, SMS OTP and tan lists (pre-printed OTPs) should be avoided as they would seem to fail the EBA guideline tests.

SOURCES

Final Guidelines on the Security of Internet Payments, EBA 19 Dec 2014 [EBA/GL/2014/12]

Consultation Paper on implementation of EBA Guidelines on Security of Internet Payments, EBA 20 Oct 2014 [EBA/CP/2014/31]

Assessment Guide for the security of Internet Payments, ECB Feb 2014

ECB Recommendations for the Security of Internet Payments, ECB Jan 2013 (aka "SecuRe Pay")

Payment Services Directive, 13 Nov 2007 [2007/64/EC]


VERISEC