EBA Guidelines

How to handle EBA Guidelines on internet payment security to prepare PSD2

Olivier Maas,
R&D Manager, expert in payment security

Definitions

ACS: Access Control Server

EBA: European Banking Authority; the European banking supervisory authority, established by means of Article 16 of Regulation (EU) No. 1093/2010

PSP: Payment Service Provider, defined as anyone covered by the requirements set out in the Payment Services Directive [2007/64/EC]

OTP: One-time password

PSD2: 2nd Payment Service Directive

Strong customer authentication: Defined in EBA Guidelines as a procedure based on the use of two or more of the following elements – categorized as knowledge, ownership and inherence:

1. something only the user knows, e.g. static password, code, personal identification number;
2. something only the user possesses, e.g. token, smart card, mobile phone;
3. something the user is, e.g. biometric characteristic, such as a fingerprint.

Refer to paragraph 12 of the EBA Guidelines for the full definition.

What are the EBA Guidelines about?

The ***European Banking Authority's (EBA) Guidelines*** are regulatory requirements applicable to financial institutions across the EU. As the security requirements under the revised Payments Services Directive (PSD2) are not expected to come into force until 2018/9, the EBA has issued its Guidelines on the security of internet payments to bridge the period of the PSD2 finalization. The requirements are a response to increases in fraud that regulators have observed with internet payments. The Guidelines set out common security requirements for payment services providers across the EU, and provide enhanced protection of EU consumers against payment fraud on the Internet.

The requirements cover a range of security measures applicable to PSPs:

- Risk management: security policies implementation and review. These should include a formal risk assessment, control and mitigation, monitoring and traceability;
- Customer awareness, education and communication;
- Specific control and security measures applicable to the initiation of internet payments - the main measure being strong customer authentication.

The Guidelines affect cards, credit transfers, e-mandate and e-money. They exclude:

- payments where the instruction is given by post, telephone order, voicemail;
- mobile payments other than browser-based ones;
- card payments using anonymous and non-reloadable cards or virtual pre-paid cards;
- browser-based payments done with mobile wallets.

What is the status of EBA Guidelines? Are they mandatory?

The Guidelines are based on the «comply or explain» principle, which means that national authorities have to notify the EBA whether they will comply with the Guidelines or otherwise explain their reason for non-compliance. Most EU countries have confirmed their compliance with the Guidelines on the security of internet payments, which are now in place - since August 1st, 2015. The EBA has made available a summary table of the compliance notifications received. Not being compliant clearly means putting business at risk.

The term 'Guidelines' is somewhat misleading since it may seem to indicate non mandatory 'best practices'. This is clearly not the case. So, as the Guidelines do not create binding law, the EBA has asked all European competent authorities to confirm their compliance and has published their answers in ***The Compliance Table.***

EBA Guidelines

Why is strong customer authentication the main measure and why is it so important to implement?

Strong customer authentication is the key requirement of EBA Guidelines because it is the most efficient measure to fight against fraud, reinforce trust in the internet payment ecosystem and protect sensitive data.

The EBA Guidelines define strong authentication as multi-factor authentication (see the definition section), with a set of additional requirements:

1. **A minimum of two authentication factors:** this is the basic requirement. Security based on a password (one knowledge factor) must now be complemented with a second authentication factor, be it a physical object or a biometric characteristic. Solutions relying solely on passwords are excluded, as are solutions relying on simple generators of one-time passwords.
2. **Mutually independent factors:** this requirement means that the vulnerability of one factor of authentication should not compromise the second factor. Typically, solutions combining knowledge and possession factors with weak protection do not meet this requirement.
3. **At least one non-reusable and non-replicable factor:** this requirement applies to the ownership factor: it means that it should be impossible to duplicate the hardware token. Pre-computed and/or pre-printed lists of OTPs do not comply with this requirement.
4. **Limited time validity of OTPs:** OTP should have a limited time validity to avoid them being stolen and reused.
5. **Authentication data confidentiality:** communications must be secured and eventually anti-malware solutions should be implemented on devices. Unencrypted SMS OTP solutions do not comply with this requirement.

Overall, the EBA Guidelines rule out a number of existing authentication methods: beyond static passwords, grid cards and non-secure OTP generators used without a second authentication factor do not comply. Appropriate answers to these strict requirements can be found in out-of-band strong authentication solutions embedded in users' personal devices or on separate hardware solutions.

How can banks move forward?

The issuance of the EBA Guidelines has accelerated the deployment of strong authentication solutions and we expect even more acceleration until the final implementation of the PSD2. This deployment takes time because it needs to be done for all payment methods within the scope – affecting digital commerce and banking – but also all interaction channels – web, mobile, etc.

Still, the EBA Guidelines open the door to more nuanced approaches: for low risk transactions, the Guidelines acknowledge that weaker authentication solutions can be adopted. RBA - Risk Based Authentication – provides answers to this approach, although, again, it is not trivial to deploy RBA across all interaction channels and impacted business area.

Finally, a key element to effectively securing payments is to empower customers. This will involve them in concrete terms and allow them to contribute to the security of their payment methods. For instance, banks can offer their clients clever ways to set spending limits on their payment methods, restrict usage to specific trusted devices, specific trusted places, times, etc.

What does Worldline offer to support banks in these new challenges?

Security challenges have always been at the heart of Worldline concerns and our clients can rely on our more than 40 year expertise to meet these regulatory requirements. Worldline offers proven solutions, such as our ACS platform, to implement 3-D Secure with risk-based approach, many trusted authentication methods for the required Strong Customer Authentication and even a payment modulator to empower the end user when it comes to controlling their payments.

And yet security is not just a question of tools. It is also a real strategy. That's why you can assign our experts to assess your fraud risk and to provide you with the most efficient recommendations.

Building trust is a long and difficult process. As the European leader in ePayment services, Worldline is ready and willing to make contributions at any time and on any channel with a view to strengthening security in the digital transactions between you and your clients.

Sources

EBA Guidelines
EBA Compliance Table
EBA press release from December 2014
EBA Compliance table

About Worldline

Worldline [Euronext: WLN] is the European leader in the payments and transactional services industry. Worldline delivers new-generation services, enabling its customers to offer smooth and innovative solutions to the end consumer. Key actor for B2B2C industries, with over 40 years of experience, Worldline supports and contributes to the success of all businesses and administrative services in a perpetually evolving market. Worldline offers a unique and flexible business model built around a global and growing portfolio, thus enabling end-to-end support. Worldline activities are organized around three axes: Merchant Services & Terminals, Mobility & e-Transactional Services, Financial Processing & Software Licensing. Worldline employs more than 7,300 people worldwide and generated 1.15 billion euros revenues in 2014. Worldline is an Atos company.

For further information
infoWL@worldline.com

FSC
www.fsc.org
The mark of responsible forestry