PAS 499:2019

Code of practice for digital identification and strong customer authentication

midas alliance

bsi.

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

Published by BSI Standards Limited 2019.

ISBN 978 0 580 94481 9

ICS 03.060; 35.240.15; 35.240.40

Publication history

First published July 2019

Contents

Foreword

This PAS was sponsored by the MIDAS Alliance (Mobile IDentity Authentication Standard). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 31 July 2019.

Acknowledgement is given to the following organizations that were involved in the development of this PAS as members of the steering group:

- AirPlus International Ltd.
- Barclays Bank UK PLC.
- BT Group plc
- Cabinet Office
- Citibank
- Co-opted
- BSI Consumer & Public Interest Network (CPIN)
- Experian Ltd.
- Facebanx
- Global Cyber Alliance
- Huntswood CTC Ltd.
- Lloyds Banking Group Plc
- Mk2 Consulting Limited
- Mobile IDentity Authentication Standard Alliance (MIDAS)
- National Cyber Security Centre (NCSC)
- Tax Incentivised Savings Association (TISA)
- Vendorcom Ltd.

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a code of practice to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or to constitute part of the UK input into the development of a European or International Standard.

Use of this document

As a code of practice, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this PAS is expected to be able to justify any course of action that deviates from its recommendations.

Relationship with other publications

The PAS builds on existing standards, directives and regulations, and provides additional recommendations and guidance to those seeking regulatory or legislative compliance.

PAS 499 relates to BS 8626, *Code of practice for the design and operation of online user identification systems* (currently in development, expected publication in 2020). PAS 499 focusses on the management principles and regulatory view of identification and strong customer authentication, with a focus on the Second Payment Services Directive (PSD2) while BS 8626 provides a framework to help organizations design and implement the technical systems/approaches for user identification.

Presentational conventions

The provisions of this code of practice are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. "organization" rather than "organisation").

The word "should" is used to express recommendations of this PAS. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

Particular attention is drawn to the following specific regulations:

- DIRECTIVE (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [1]
- Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication [2]
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [3]
- DIRECTIVE (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union [4]
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [5]

0 Introduction

0.1 Background to the PAS

Cybercrime and fraud are the fastest growing areas of criminal activity, and vulnerabilities in identity and authentication practices account for much of this unwelcome growth. Adoption of robust digital identity and strong customer authentication processes are essential to minimizing the risks to organizations and their users, employees and partners, associated with online transactions and services that a successful digital economy needs. Regulatory changes recognize these requirements, but the development of standards to meet them is vital to ensure a coherent environment for businesses, public services and users.

Digital identification and authentication systems allow organizations to manage a wide range of digital services securely (e.g. for electronic payments), but the evolving complexities of the regulatory environment makes standards crucial in helping organizations understand what is expected of them in offering such secure systems.

This PAS does not seek to replicate legislation and relevant guidance. This PAS sets out recommendations for organizations to meet security, regulatory, and usability requirements in the provision of digital services in line with requirements of the Second Payment Services Directive (PSD2) [1]. It aims to assist organizations in understanding changes to existing security practices necessary to prevent fraud techniques that have evolved, or could be developed, to circumvent controls.

0.2 Digital identification and the aims of the PAS

In the online world the process to identify users at enrolment, and subsequently authenticate that it is genuinely the user returning, is a core underlying requirement necessary for a myriad of day to day functions in public and commercial life. This PAS provides recommendations to take into account when implementing strong customer authentication in line with PSD2 [1]. Some of these recommendations might apply in other contexts, such as accessing online services, providing explicit consent under subject access rights, or any number of other services. For example helping organizations check that a user has the right to work or rent accommodation.

Equally, the ability to build up a picture of an otherwise hard to categorize segment of society means that this PAS offers possible security solutions to mitigate problems such as "banking the unbanked" or providing a first step to documenting the undocumented.

This PAS covers good practices for an organization's identification and authentication processes building on lessons learned from experience and analysis of current and emerging cyber security threats, such as those identified under the Network Information Systems Directive [4] and from other stronger sector specific security standards in payment security.

It aims to help organizations secure their systems to reduce the incidence of fraudulent misrepresentation of a natural or legal person. It also provides recommendations and guidance on other elements to be considered in the design of a process to optimally implement a system to meet legal requirements.

It builds on:

- existing standards, directives and regulations to provide additional recommendations and guidance, taking into account new regulatory security requirements, to address cybercrime trends; and
- developments in the move towards, but not limited to, combined financial and government identity and authentication requirements; this may, for example, include commercial applications for notified schemes under the electronic identification, authentication and trust services (eIDAS) Regulation [3].

This PAS seeks to assist organizations to implement practices to manage identification and authentication. However, since these practices are specific to the operational context of the implementation, these practices are not considered in this PAS.

0.3 Existing standards, legislation and guidance

Data protection requirements and enforcement powers have been greatly increased by the General Data Protection Regulation (GDPR) [5], whilst in payment services PSD2 [1] raises the regulatory requirements on authentication from a low baseline to a strong user authentication, where security requirements might go beyond that expected in other sectors.

Existing standards and guidelines, such as the Good Practice Guide (GPG) 45, Identity Proofing and Verification of an Individual [6]; the National Institute of Standards and Technology (NIST) 800-63-3 Digital Identity Guidelines [7]; PD ISO/IEC TR 29196; and underlying information security standards, such as the ISO/IEC 27000 series, are the backdrop on which PAS 499 seeks to build.

Whilst explanatory documents exist that clarify some of the component parts of such existing standards, directives and regulations, such as guidance on the enrolment of biometric authentication factors included in PD ISO/IEC TR 29196 and Joint Money Laundering Steering Group (JMLSG) [N1] guidelines for financial services businesses on identity verification, there is no encompassing, end-to-end guidance that puts identification and authentication in context and outlines an approach to assisting with regulatory or legislative compliance. This PAS notes PD ISO/IEC TR 29196 and its guidance on biometric enrolment, and the importance of capturing a more extensive range of biometrics both for user choice and experience and to help establish uniqueness due to the issue of false positives in each biometric modality.

The UK government has published GPG 45 [6] intended to inform government departments and suppliers of good practice in establishing levels of identity assurance. This PAS builds on this document and on the good practice recommendations for security it sets out.

The JMLSG guidance [N1] is derived from the EU Money Laundering Directives [8] which are themselves driven by the requirements of the Financial Action Task Force (FATF) [9]. Such anti-money laundering guidance is sometimes seen as an inhibitor for citizens in some demographic groups or categories, such as asylum seekers, to establishing an identity in order to open an account, but who are still required to be strongly authenticated were they able to open an account (see Annex A for use cases).

The International Organization for Standardization (ISO) covers the area of digital identity in a number of standards, for example BS PD ISO/IEC TS 29003 and BS ISO/IEC 29115. By referencing the emerging regulatory standards, this PAS brings together and proposes a resolution for some of the conflicting terms in these standards and in the new regulatory environment with a replacement to the definitions contained in BS ISO/IEC 24760-1, which relate to the authentication of all types of entity and not persons specifically.

In the United States, NIST has also published guidance, such as 800-63-3 [7] on the use of electronic identification and authentication. Given the global nature of digital identification and authentication requirements, this international dimension has been borne in mind during the development of this PAS.

This PAS gives recommendations in order to help organizations with their application of the eIDAS Regulation [3], and its definitions of "levels of assurance" and PSD2 [1] with its emerging practices of strong customer authentication to conform to GDPR [5].

1 Scope

This PAS gives recommendations for, and is for use by, all organizations requiring identification and authentication for digital activities in the context of regulatory requirements for defined levels of identification assurance and strong customer authentication, as required in the Second Payment Services Directive (PSD2) and related regulations.

NOTE 1 *The term customer is a specific instance of user.*

This PAS covers the management operations relating to systems for identification and strong customer authentication for regulated industries, including:

- identity validation;
- identity verification;
- enrolment;
- authentication;
- delegated authority and authorization;
- security and usability; and
- risk models for authentication.

This PAS also applies to management processes for creating, accessing or managing accounts digitally; users making a payment via a mobile device or other computer; users making a contactless payment using an electronic device; a retailer receiving such payments; third-party roles; delegated authority; and a bank or payment service provider administering such transactions.

It includes supporting guidance as informative annexes to the PAS including: use cases to address common scenarios and strong customer authentication (see Annex A); and a summary description of additional good practice that can be used in developing a compliant secure system (see Annex B).

The PAS does not cover: contactless payments made using plastic cards; transactions in the context of the internet of things; digital currencies; specifics of payment devices or payment terminals.

NOTE 2 *There is a difference in the way that the term "identification" is used in this PAS (establishing an association between a known identity and a person) and that employed in biometric standards (process of searching a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single person). When used in PAS 499, the latter meaning is referred to as "biometric identification".*