BS 8626:2020

BSI Standards Publication

Design and operation of online user identification systems — Code of practice

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 2020

ISBN 978 0 5 9 01297 2

ICS 5.24 .01, 35.030

The following BSI references relate to the work on this document:
Committee reference IST/33/5
Draft for comment 20/30379129 DC

Amendments/corrigenda issued since publication

Date	Text affected

Contents

Summary of pages
This document comprises a front cover, and inside front cover, pages i to iv, pages 1 to 115, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 December 2020. It was prepared by Subcommittee IST/33/5, *Security techniques — Identity management and privacy technologies*, under the authority of Technical Committee IST/33, *Information security, cybersecurity and privacy protection*. A list of organizations represented on these committees can be obtained on request to the committee manager.

Relationship with other publications

PAS 499:2019, *Code of practice for digital identification and strong customer authentication*, covers the management operations for identification and strong customer authentication, as required in the Second Payment Services Directive (PSD2) [1] and related regulations. BS 8626 provides recommendations to digital identity providers, including relying parties, covering the establishment of requirements for online user identification systems and their design and management operations.

The recommendations contained in PAS 499:2019 will be reviewed and incorporated into the next edition of BS 8626.

While the ISO/IEC 24760 series specifies concepts and operational structures of identity management for entities in general, BS 8626 concentrates on the processes for managing digital identities for the sole purpose of online user identification. BS 8626 also provides recommendations on the use of knowledge-based and possession-based authentication methods and, additionally, biometric recognition methods for user identification, together with recommendations for managing the effectiveness and efficiency of deployments.

Information about this document

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at bsigroup.com/standards, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Use of this document

As a code of practice, this British Standard 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 British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The provisions of this standard 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.

The word "should" is used to express recommendations of this standard. 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.

Notes and commentaries are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

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

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 British Standard cannot confer immunity from legal obligations.

Introduction

This British Standard uses the term "identification" in a general sense for the online recognition of individuals, as authorized users, by digital identity providers (IdPs) working with relying parties (RPs) that supply online services. In many cases the RP and the IdP are part of the same legal entity, although the operation of the online user identification system (OUIS) can be managed by a different department within that organization or by an entirely separate entity. This standard also uses and defines terms, such as identity proofing, authentication, verification, recognition and biometric identification, as specific types of identification processes.

Society and organizations are increasingly dependent on online information systems providing services which on access to restricted resources, such as sensitive data and controlled functions. These services, operating in diverse contexts, are provided by a range of entities, which include governmental, educational, commercial and charitable RPs. The services available today are pervasive, providing, for example, functionalities to users to manage personal tax information, accountants to send corporate tax communications, college administrators to distribute student course materials, consumers to purchase goods and services, customers to conduct online banking activities, customers to reserve hotel accommodation, and citizens to submit donations to charities.

Organizations providing user identification services need to ensure that access to these restricted resources is provided to the relevant authorized users, such as citizens, customers, consumers or employees, in an effective and efficient manner. Key to delivering this requirement is selecting the optimal access control systems so that the stakeholder benefits, including rewards to the intended user community, are realized and that the concomitant risks are managed by these parties in an informed, transparent and equitable manner. To meet these challenges, organizations need to balance complementary and conflicting stakeholder objectives; consider interrelated factors, such as cost containment, productivity impact, usability, accessibility, sustainability and performance; and evaluate user identification assurance.

To manage risks, RPs employ online user authentication methods and/or biometric recognition methods utilizing one or more types of user identification data and modes of operation to identify a user to a predetermined level of assurance. An RP can specify and manage the user identification processes for its own customers, e.g. banks, which utilize its services. RPs assess and manage risks directly. Alternatively, an RP can utilize a third-party digital identity provider (IdP) to manage its user identification processes. In this federated model, the IdP specifies the technical and process requirements and manages the user identification processes with any RPs, as part of its access control procedures for the RPs' online services. In these circumstances for the relevant application context, IdPs and possibly other organizations provide an input into an RP's assessment and management of risk. Multiple authentication methods and/or biometric recognition methods can be deployed for user identification, either to be used together to strengthen the assurance in determining the identity of the user to access the RP's service, or as user identification alternatives, if significant numbers of users are unable to use an authentication method and/or biometric recognition method in a reliable manner.

All user identification systems incur costs, both direct and indirect, possess technical and procedural vulnerabilities, and potentially attract deleterious intractable issues. Organizations face complex challenges in ascertaining their optimal user identification system and managing it for their applications in an online operating environment with ever-increasing threats, competition and regulation. This British Standard gives recommendations and guidance for resolving these challenges.

The recommendations in this standard are intended for organizations seeking to introduce an OUIS as part of the design for a new application service or a revision to an operational deployment.

The standard commences with recommendations for selecting or enhancing current user identification systems and then gives recommendations for the three main types of user identification system, knowledge-based authentication, possession-based authentication and biometric recognition methods. A clause on contra-indicators sets out the recommendations for using additional data to support the methods deployed in order to acquire confirmatory evidence or identify the possible compromise of user identification. The recommendations in Clause 5 on digital identity life cycle management are then applicable based upon the types of methods deployed. The final clauses give general recommendations for managing user identification systems and supporting digital identity management systems (IdMS).

1 Scope

This British Standard gives recommendations and supporting guidance for the design and operation of an online user identification system (OUIS) and the corresponding user digital identity management systems (IdMS). As authorized users, individuals can act in a personal capacity (e.g. consumer, customer or citizen) or on behalf of another individual (e.g. as a proxy) in a role in a digital identity provider (IdP) and/or relying party (RP), e.g. employee or authorized contractor. In particular, recommendations are given for:

a) establishing or revising an OUIS, including:

   1) business objectives and requirements for an OUIS;

   2) requirements for protecting the life cycle management of digital identities associated with individuals;

   3) requirements for protecting data used specifically for identifying or authenticating individuals;

   4) requirements for protecting against attacks on specific types of user knowledge-based authentication methods, possession-based authentication methods and biometric recognition methods and modes of operation;

b) the controls for managing the life cycle of users' digital identities for an OUIS, including:

   1) creation, proofing and issuance of a digital identity and the formation of the digital identity's associated credential;

   2) identification together with credential usage (where applicable);

   3) activities to update credentials and associated data, and notification of these changes to the user;

   4) revocation, expiration, reinstatement, disqualification or user cancellation of a digital identity's credential and purging or archiving of digital identities; and

c) evaluating the effectiveness of an OUIS, including the management of user identification errors, such as false positives and false negatives, and efficiency, including the user identification transaction timings and demand on resources.

This British Standard:

i) describes various knowledge-based authentication methods, possession-based authentication methods and biometric recognition methods, together with their inherent vulnerabilities;

ii) provides recommended measures to mitigate the potential exploitation of these identified vulnerabilities; and