October 2014
Issue No: 2.0

Good Practice Guide No. 44

Authentication and Credentials for use with HMG Online Services

CabinetOffice

CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Good Practice Guide No. 44

Authentication and Credentials for use with HMG Online Services

Issue No: 2.0
October 2014

This document is issued jointly by CESG, the UK's National Technical Authority on Information Assurance and Cabinet Office, Government Digital Services. It is provided "as is" as an example of how specific requirements could be met, but it is not intended to be exhaustive, does not act as endorsement of any particular product or technology and is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take the appropriate technical and legal advice in using this document.

Document History

Version	Date	Comment
1.0	April 2012	First issue
1.1	December 2012	Updated to incorporate comments received from HMG Departments. Minor changes made to align with terminology used in GPG 45
1.2	May 2013	Updated the description of Table 5 and other general formatting improvements
2.0	October 2014	Second issue

Purpose & Intended Readership

The purpose of this document is to provide good practice guidance to HMG public service providers and their service providers (e.g. Identity Service Providers) on the use of identity credentials to support user authentication to HMG Online Services. This document is intended to compliment and support the guidance provided in CESG Good Practice Guide No. 45 (GPG 45), Identity Proofing and Verification of an Individual (reference [a]).

This document will primarily describe how types of credentials support the authentication levels, with further information on other elements to be considered. Additional background information is provided in the Annexes.

Executive Summary

Delivery of an online public service may attract significant levels of risk, as it will present a very attractive target for many sources of threat. Public sector service providers should make informed choices with regard to credentials that support the upper 3 (of the 4) levels of authentication, related to HMG Online Services, that have controls defined. The value of an authentication credential, and hence the level of assurance assigned to it, is determined by many different elements, which can be characterised under the following 6 headings:

- The type of credential required for a given authentication level
- The quality factors related to a credential
- The quality of the ongoing management of the credential by the Identity Provider (IDP)
- The extent and quality of monitoring, and reactions, by the IDP and the credential manufacturer
- The authentication service characteristics that protects the user, and itself, from compromise
- The Information Assurance maturity of the authentication provider

These elements should be considered against the threat landscape associated with the Government service provider and that of the IDP. In some instances, the threat landscape directly associated with the IDP's own services (e.g. banking) may present a higher set of risks than those associated with the public service provider. The underlying outcomes still need to be achieved in all these cases.

Changes from Previous Issue

This issue is a complete replacement of the previous version 1.2 guidance. It has moved its emphasis to outcomes, rather than specific techniques, to help encourage adaptability in an environment of evolving threats.

Feedback

CESG Information Assurance Standards and Guidance welcomes feedback and encourage readers to inform CESG of their experiences, good or bad in this document. Please email: enquiries@cesg.gsi.gov.uk

Contents:

Chapter 1 - Introduction

Key Principles

- Alignment with National and International Standards, including GPG 43, RSDOPS, (reference [b])
- Level 0 (RSDOPS lowest level) authentication does not have associated controls
- Outline of the upper level (Level 1 to Level 3) authentication outcomes

Levels of Authentication

1. This guide has been written with the intention of being aligned with National and International Standards, including GPG 43, RSDOPS (reference [b]) which describes the levels of Authentication. It should be noted that not all the security characteristics in GPG 43 RSDOPS (reference [b]) require controls at Level 0, and authentication is one such characteristic.

Level 1 Authentication

2. The authentication demonstrates that the person requesting authentication is in possession of the Credential for a legitimate account. At this level, it is not necessary to link the use of the Credential to the owner, therefore there is no protection against Credential theft.

Level 2 Authentication

3. The authentication provides sufficient confidence that the Credential is being used by the legitimate account holder, or with the explicit consent of the legitimate account holder, and might be offered in support of civil proceedings. The Credential is bound to its owner and provides protection against Credential theft.

Level 3 Authentication

4. The authentication provides sufficient confidence that the Credential is being used by the legitimate account holder, or with the explicit consent of the legitimate account holder, and might be offered in support of criminal proceedings. The Credential is bound to its owner and protects the transaction from attacks where the Credential may have been compromised.

Chapter 2 - Minimum Authentication Outcomes

Key Principles

- There are six authentication credential characteristics
- Each of the authentication levels have sub-elements describing the requirements for that level

Minimum Outcome by Level

5. This Chapter sets out the minimum outcomes that are expected when Credentials are used to support authentication to HMG online services. Where a term/acronym is unknown, then the Glossary, after the annexes, may help.

6. The following minimum scores are expected for Authentication levels 1-3, in accordance with Chapter 1, for each of the Authentication and Credential (AC) elements:

- **Level 1 -** A minimum score of 1 is expected for each of the AC elements
- **Level 2 -** A minimum score of 2 is expected for each of the AC elements
- **Level 3 -** A minimum score of 3 is expected for each of the AC elements

AC Element A: Credential Type

7. It is considered that the following Credential types, and combination of Credential types, are appropriate to support each of the authentication levels. The following table demonstrates the type of Credential required in order to meet the authentication levels set out in Chapter 1.

Score	Credential Type
1	• A Credential type that demonstrates the user is in possession of a Secret (e.g. a password, PIN, etc.) belonging to the legitimate account holder (see Annex A for further guidance on Secrets).
2	**Requirements for Score 1, plus <u>one</u> of the following:** • A Credential type that demonstrates the user is in possession of a Secret (e.g. a password, PIN, OTP, LTS, etc) belonging to the legitimate account holder that is exchanged over a channel that is separate to the authentication channel (see Annex A for further guidance on Secrets). • A Credential type that demonstrates the user is in possession of a biometric belonging to the legitimate account holder (see Annex D for further guidance on the use of biometrics).
3	**Requirements for Score 1, plus the following:** • A Credential type that demonstrates the user is in possession of a hardware or software token belonging to the legitimate account holder.

Table 1 - Credential Types

AC Element B: Quality of the Credential

8. The effectiveness of measures that the Credential employs to protect it from being predicted, duplicated or otherwise compromised are important factors in assessing its suitability for use. The following Table demonstrates the properties for the quality of the Credential and the corresponding score for this element. The Credential must, as a minimum, meet all the properties defined for the quality to achieve that score.

Score	Quality of the Credential
1	• The Credential contains no protective measures to prevent prediction or duplication (e.g. it is a Secret that is memorised by the user). • Users shall be encouraged through process, or guidance, to use Credentials with good security properties.
2	• The Credential uses measures that make it unlikely to be predicted. • The Credential has measures that prevent duplication without direct access to the Credential. • The Credential has measures that resist tampering. • Hardware and software tokens are implemented in accordance with current Good Industry Practice (e.g. NIST SP 800-63-2, (reference [c])) including protection against offline attack. • Cryptographic modules used have been assessed as using algorithms and security measures in accordance with Good Industry Practice (e.g. FIPS 140-2 Level 2,(reference [d])).
3	**Requirements for Score 2, plus the following:** • The Credential has measures that prevent duplication. • The Credential has measures that detect and prevent compromise from tampering. • Cryptographic modules used have been assessed as using algorithms and security measures in accordance with Good Industry Practice (e.g. FIPS 140-2 Level 3, (reference [d])).

Table 2 – Quality of the Credential

AC Element C: Management of the Credential

9. The confidence in the Credential is not only dependent on its properties, as the Authentication Provider must carefully manage the Credentials over their lifetime. The following Table demonstrates the required Credential management processes and the corresponding score for this element. The Authentication Provider must, as a minimum, meet all the properties defined for Credential management to achieve that score.

Score	Credential Management
1	• The Authentication Provider stores Credentials so that they are protected from unauthorised physical and electronic access to prevent theft or damage. Further information on the storage of Credentials can be seen at Annex C. • The Authentication Provider shall be able to suspend a Credential immediately from the primary system that stores the records of the currently authorised Credentials. • The Authentication Provider shall be able to permanently revoke a Credential with immediate effect. • The Authentication Provider shall enable the user to recover/request a replacement Credential. • The Authentication Provider shall ensure that changes to the state of the Credential requested by the user can only be made by the person to whom the Credential belongs. • The Authentication Provider shall ensure the Credential is bound to a single account. • The issuing process for the Credential shall take measures that attempt to deliver it into the possession of the user that requested it. • The Authentication Provider shall ensure that the Credential is under the control of the person/user to whom it belongs before, or on, first use. • Where the Credential has been manufactured, the manufacturer shall have a quality management process to ensure consistency. • Where the Credential uses information embedded by the manufacturer (e.g. secret number), the manufacturer shall have an information security management system which protects that information from compromise (e.g. ISO27001, (reference [e])). • Where a Credential manufacturer supplies information to the Authentication Provider, which is required as part of the Authentication, then the process for exchanging that information shall protect its integrity and confidentiality.
2	**Requirements for Score 1, plus the following:** • The issuing process for the Credential shall take sufficient measures so that it **can reasonably be assumed** to have been delivered into the possession of the person to whom it belongs. • Where the Credential has been manufactured, the manufacturer shall have an **independently audited** quality management process to ensure consistency (e.g. ISO 9000 series, (reference [f])). • Where the Credential uses information embedded by the manufacturer (e.g. secret number), the manufacturer shall have an **independently audited** information security management system which protects that information from compromise (e.g. ISO 27001, (reference [e])).
3	**Requirements for Scores 1 and 2, plus the following:** • The issuing process for the Credential shall **take all reasonable measures to ensure** it has been delivered into the possession of the person to whom it belongs. • Where the Credential has been manufactured, the manufacturer shall have an **independently certified** quality management process to ensure

Score	Credential Management
	consistency under a Good Industry Practice certification scheme (e.g. ISO 9000 series, (reference [f])). • Where the Credential uses information embedded by the manufacturer (e.g. secret number), the manufacturer shall have an **independently certified** information security management system which protects that information from compromise (e.g. ISO 27001, (reference [e])).

Table 3 – Management of the Credential

AC Element D: Monitoring

10. The qualities and management of the Credential contribute to its security, but it is also necessary to monitor its use. Therefore, the Authentication Provider shall monitor the use of a Credential, its services and sources to detect and react (e.g. incident management) to the misuse of a Credential. The following table demonstrates the monitoring requirements and the corresponding scores for this element. The Authentication Provider must, as a minimum, meet all the properties defined for monitoring to achieve that score.

Score	Monitoring
1	• The Authentication Provider shall check for indications that the Credential maybe being used by someone other than its owner. • Where the Authentication Provider has reasonable suspicion that the Credential is being used by someone other than its owner, the Authentication Provider shall take sufficient measures in order to determine the user is the owner of the Credential, which may include revoking and replacing the Credential.
2	**Requirements for Score 1, plus the following:** • The Authentication Provider shall take measurements to establish what normal and legitimate authentication behaviour looks like (see CESG Good Practice Guide 53 (GPG 53), Transaction Monitoring for HMG Online Service Providers, (reference [g])). • The Authentication Provider shall detect, and where applicable report, abnormal authentication behaviour (see GPG 53, (reference [g])).
3	**Requirements for Scores 1 and 2, plus the following:** • The Authentication Provider shall check HMG provided services for indications that the Credential maybe being used by someone other than its owner.

Table 4 – Monitoring

AC Element E: Authentication Service Characteristics

11. Confidence in the use of a Credential, during the Authentication, is built upon the characteristics of the authentication service. The Authentication Provider shall ensure its authentication service protects the user, and itself, from compromise. The following Table demonstrates the required characteristics of the authentication service and the corresponding score for this element. The

Authentication Provider must, as a minimum, meet all the properties defined for the authentication service characteristics to achieve that score.

Score	Authentication Service Characteristics
1	• The Authentication Provider shall design, develop, implement and maintain the technology systems that deliver its authentication services to protect the confidentiality, integrity and availability of the information processed. • The Authentication service shall only return a success where the user has successfully authenticated using their Credential. • The Authentication service shall reject an Authentication when a suspended or revoked Credential is presented. • The Authentication service shall suspend or revoke a Credential after a number of failed Authentication attempts. • The Authentication service shall protect authentication sessions using Good Industry Practice security measures to ensure its confidentiality, integrity and authenticity and provide non-repudiation (e.g. using TLS v1.2 (reference [h]), digital signatures FIPS 186-4 (reference [i]), etc.). • The Authentication service shall ensure that the user can determine that they are using a secure channel to the Authentication Provider (e.g. where certificates are being used, then these are not self-signed but are signed by an industry recognised authority). • Where the Authentication service uses cryptography, then the cryptographic algorithms and keys shall be used in accordance with current Good Industry Practice. For further information, see Annex B.
2	**Requirements for Score 1, plus the following:** • The Authentication Provider shall use measures that are effective at preventing use by non-human operators (see Good Practice Guide 53, (reference [g])). • The Authentication service shall use measures that prevent the observation and replay of Credentials that were used in a previous Authentication. • The Authentication service shall use methods that ensure the integrity of the information exchanged with a user. • The Authentication service shall use measures that protect the Credential from compromise, even if the communication channel is compromised.
3	**Requirements for Scores 1 and 2, plus the following:** • The Authentication service shall use measures that detect and prevent the illegitimate use of a user's Credential.

Table 5 – Authentication Service Characteristics

AC Element F: Information Assurance Maturity of the Authentication Provider

12. The information assurance maturity of the Authentication Provider is an important element in providing confidence in the delivery of the authentication service. The following Table demonstrates the information assurance maturity requirements for the Authentication Provider and the corresponding score for

this element. The Authentication Provider must, as a minimum, meet all the properties defined for the information assurance maturity to achieve that score.

Score	Information Assurance Maturity
1	• The Authentication Provider shall have an effective information security management system which protects the integrity, confidentiality and availability of its service including a forensic readiness plan. • The Authentication Provider shall have an audit regime that covers all systems supporting the use of the Credential. • The Authentication Provider shall ensure that all systems supporting the use of the Credential have a consistent time. • The Authentication Provider shall have a records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential. • The Authentication Provider shall conduct regular risk assessments and have defined processes for exception handling. • The Authentication Provider shall have a monitoring regime that detects unexpected and undesirable activity within the service. • The Authentication Provider shall have an internal monitoring regime that detects unusual, or malicious, activity of the Authentication Provider's staff and others that have physical and logical access to the systems that support the authentication service.
2	**Requirements for Score 1, plus the following:** • The Authentication Provider shall have an **independently audited** information security management system which protects the integrity and confidentiality of its service (e.g. ISO27001, (reference [e])), including a forensic readiness plan. • The Authentication Provider shall have an **independently audited** audit regime that covers all systems supporting the use of its service, including a forensic readiness plan. • The Authentication Provider shall ensure that all systems supporting the use of the Credential have a consistent accurate time using a Good Industry Practice time source. • The Authentication Provider shall have an **independently audited** records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential. • The Authentication Provider shall conduct regular risk assessments, and have defined processes for exception handling, using Good Industry Practice guidance (e.g. ISO 27005, (reference [j])). • The Authentication Provider shall have an **independently audited** monitoring regime that detects unexpected activity within the service. • The Authentication Provider shall test its monitoring regime through a schedule of independent vulnerability and penetration tests, adjusting it to address any issues discovered. • The Authentication Provider shall have an **independently audited** internal monitoring regime that detects unusual, or malicious, activity of the Authentication Provider's staff and others that have physical and

Score	Information Assurance Maturity
	logical access to the systems that support the authentication service. • The Authentication Provider shall test its internal monitoring regime through a schedule of independent vulnerability and penetration tests, adjusting it to address any issues discovered.
3	**Requirements for Scores 1 and 2, plus the following:** • The Authentication Provider shall have an **independently certified** information security management system which protects the integrity and confidentiality of its service (e.g. ISO 27001, (reference [e])), including a forensic readiness plan. • The Authentication Provider shall have an **independently certified** audit regime that covers all systems supporting the use of the Credential (e.g. ISO 27001, (reference [e])). • The Authentication Provider shall ensure that all systems supporting the use of the Credential have a consistent and accurate time synchronised from a Stratum 1 time source (or equivalent). • The Authentication Provider shall have an **independently certified** records management system for identifying, classifying, prioritising, storing, securing, archiving, preserving, retrieving, tracking and destroying of records that covers all systems supporting the use of the Credential (e.g. ISO 15489, (reference [k])).

Table 6 – Information Assurance Maturity

13. Threat sources and threat actors should be considered in the context of the online service involved.

14. Further information on the threats, vulnerabilities and impacts, relevant to an online service, can be found in GPG 43, (reference [b]).

Annex A – Generation and Use of Credentials for Authentication

Introduction

15. Credentials, including Secrets, shall be secure from brute force attacks. This means that they shall have sufficiently high entropy. If a Credential is complex, then it is much harder for an attacker, with no inside information, to guess what it might be. This applies to Credentials used at any level, so entropy guidance depends on the Credential type.

Generation of Secrets

16. Secret information (e.g. a password, LTS) can be generated by the person who needs it, or by a system operated by, or on behalf of, the Authentication Provider. The following is a discussion of each of these, and it provides relevant guidance.

Computer Generated Secrets

17. Computer generated Secrets shall conform to a set of rules. The Authentication Provider shall ensure that any Secret will be generated with equal probability; therefore the entropy is the total number of Secrets that conform to the rules. The following Table provides an example of the required entropy, along with example rules for composition, although protection from a brute force attack may be dependent on the algorithms used to secure it (e.g. ICO MD5 hashes guidance in Appendix B of reference [l]).

Credential Replacement Period	Entropy Required	Rules for the Composition of Secrets			
		Same Case Characters	Mixed Case & Special Characters	Numeric Only	Hexadecimal Characters
≈1 year	$\approx 2^{45}$	10	8	14	12
≈1 week	$\approx 2^{39}$	9	7	12	10
≈1 day	$\approx 2^{36}$	8	6	11	9
≈15 minutes	$\approx 2^{30}$	7	5	9	8
≈1 minute	$\approx 2^{26}$	6	4	8	7

Table 7 – Entropy Requirements and Example Rules

18. When enforcing the use of complex Secrets, it is important to note that managing these Secrets, along with all the other Secrets they have for other systems, is challenging for users. Authentication Providers shall provide guidance to their customers on how to manage this situation within

recommended guidelines to avoid poor personal operating procedures that could undermine the security of the Credential.

19. In conjunction with these rules that the Authentication Provider shall follow, there is guidance given, in this document, on storing Secrets (Annex C). The above rules are only valid where the Authentication Provider follows such guidance.

User Generated Secrets

20. Humans are generally bad at generating Secrets and thus most will generate Secrets that are vulnerable to a brute-force attack. Guidelines on generation, either recommended or enforced, will alleviate this issue, but certainly will not solve it. Guidelines should be given using a strength meter or some other solution. The Authentication Provider shall enforce the same entropy guidelines as for machine generated Secrets. However, it must be accepted that human generated secrets are likely to conform to a pattern and be vulnerable to brute force attack, even under these controls.

Partial exposure of a secret during authentications

21. One way of using a Secret to authenticate is to expect the provision of a long secret, and then to ask for only certain characters from the secret at each authentication. This is an acceptable way to offer an authentication service, but usage characteristics need to be chosen with care to ensure optimal security properties.

22. Advantages of using a Credential in this way include protection of the complete Credential from a single usage on a compromised platform, e.g. on a computer in an Internet Cafe. Disadvantages include less protection against brute force attack, and the requirement to hold passwords in un-hashed form within the service architecture, and hence these related aspects :

- Care shall be taken in choosing how much, or how little, of the Credential is used per authentication, to balance the protection against brute force attack against the protection of the complete Credential
- The confidentiality of the complete Credential will quickly become compromised if repeated authentication is made on a single compromised platform
- The Credential will need to be stored un-hashed within the service architecture. This will increase the priority of the protection of this information from external attack

Use of 4-Digit PINS

23. Solutions that use 4-digit PINs to secure access to a more complex Credential, such as a cryptographic key on a smartcard, can be suitable assuming that the complex Credential meets the requirements as set out in this document.

Use of Tokens

24. Where authentication providers are using hardware or software tokens to provide an additional factor for authentication, then these shall be implemented, and managed, in accordance with the guidance provided in:

    - NIST Special Publication 800-63-2 Electronic Authentication Guideline (reference [c])

Further Guidance

25. Further information can be sought from:

    - NIST Special Publication 800-63-2 Electronic Authentication Guideline (reference [c])
    - ICO Protecting personal data in online services: learning from the mistakes of others, (reference [l])
    - Get Safe Online (reference [m])
    - Cyber Streetwise (reference [n])

Annex B – Using Cryptography

26. Further information can be sought from:

- NIST SP 800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (reference [o])
- NIST SP 800-57 Part 1 Recommendation for Key Management – Part 1: General (Revision 3) (reference [p])
- ENISA Algorithms, Key Sizes and Parameters Report 2013 recommendations (reference [q])

Annex C – Storing Secrets and Credentials within the Authentication Provider

27. There are well known attacks that have compromised databases used to store identity information and Credential information, including information that is hashed, or un-hashed, from identity provider infrastructures.

28. Authentication Provider services shall offer strong protection against such attacks. Details of this protection involve system architecture principles, and are out of scope of this paper. However the following points are all relevant, although much more will be required:

- Credentials shall be stored in hashed form only, whenever the authentication solution allows this to happen
- The Authentication Provider shall implement good security standards in relation to the storage methods including following the ICO guidance (reference [l]) on “Password storage”, “The requirements of a password hash function” and the use of a unique salt per user
- The Authentication Provider shall only use hash functions as recommended by ENISA in their recommended configurations (reference [q])
- Credentials shall be encrypted whenever being transported across a channel where it could be intercepted by someone outside of the Authentication Provider
- If a Credential is protected by cryptography, the cryptographic key shall be at least as long as the entropy required of the Credential

Annex D – Use of Biometrics

Entropy of a Biometric

29. The entropy of a biometric is both mathematically difficult to calculate and is potentially not as useful as measuring the quality of the matching process, predominantly because the most common biometrics of fingerprints and facial images have very high entropy, e.g. they are nearly unique and distinguishable amongst very large populations.

Biometric Match

30. The Authentication shall be considered successful where a recognised Good Industry Practice biometric matching process determines that the Biometric of the user matches that of the Biometric identifier used by the Credential.

31. The process by which the Authentication Provider performs the Biometric match shall be able to demonstrate that it is has a maximum False Non-Match Rate (FNMR) of 0.5% at a False Match Rate (FMR) of 0.01%, or less, based on a one-to-one comparison of a Biometric with the user (e.g. see NIST Interagency Report 8009, (reference [r]), and ISO/IEC 19795 series, (reference [s]), for further information).

32. The Biometric matching process shall use effective measures to detect the spoofing of biometric identifiers.

33. The Biometric matching process shall use effective measures to ensure that the user is not using a means of altering themselves (e.g. using makeup or prosthetics) in order to intentionally misrepresent themselves.

34. The Biometric matching process shall use effective procedural and technical measures to ensure that the Biometric presented by the user is of a real person and not an image, or other mock up.

35. The Biometric matching process shall have been independently assessed by an independent body (that is recognised within Good Industry Practice) as being able to demonstrate a high degree of accuracy in distinguishing between people of similar characteristics.

References

(Note: The CESG documents referred to in this reference should be available from the appropriate Cabinet Office Government Digital Service (GDS) pages e.g. this may be where you obtained this document, https://www.gov.uk/government/collections/identity-assurance-enabling-trusted-transactions . The other references were available at the shown locations, however if these external sites reorganise their content, you may need to search these sites to find the documents. Also, if an external site deprecates e.g. removes the content, then it may no longer be easily available after the publication of this GPG.)

[a] CESG Good Practice Guide No. 45, Identity Proofing and Verification of an Individual, Issue 2.3, July 2014

[b] CESG Good Practice Guide No. 43, Requirements for Secure Delivery of Online Public Services (RSDOPS), Issue 1.1, December 2012

[c] NIST Special Publication 800-63-2 Electronic Authentication Guideline, August 2013 (http://csrc.nist.gov/publications/PubsSPs.html)

[d] Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 2001, although the effective date was November 2001 (with change notices dated December 2002, although the annexes have later revision dates) (http://csrc.nist.gov/publications/PubsFIPS.html)

[e] ISO/IEC 27001:2013 Information Security Management Systems - Requirements[1] (http://www.iso.org)

[f] ISO 9000:2005 Quality Management Systems[1] (http://www.iso.org).

[g] CESG Good Practice Guide No. 53, Transaction Monitoring for HMG Online Service Providers, Issue 1.0, April 2013

[h] The Transport Layer Security (TLS) Protocol, Version 1.2 (RFC 5246), August 2008 (http://tools.ietf.org/html/rfc5246)

[i] Federal Information Processing Standard (FIPS) 186-4 Digital Signature Standard (DSS), July 2013 (http://csrc.nist.gov/publications/PubsFIPS.html)

[j] ISO 27005:2011 Security Techniques – Information Security Risk Management[1] (http://www.iso.org)

[k] ISO 15489:2001 Information and Documentation – Records Management[1] (http://www.iso.org)

[1] Please note that access to International Standards is on a subscription or payment basis.

[l] ICO Protecting personal data in online services: learning from the mistakes of others, version 1, May 2014 (http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Research_and_reports/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf)

[m] Get Safe Online is a jointly funded initiative between several Government departments and private sector businesses (http://www.getsafeonline.org)

[n] Be Cyber Streetwise is a cross-government campaign delivered in partnership with the private and voluntary sectors (http://www.cyberstreetwise.com)

[o] NIST SP 800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011 (http://csrc.nist.gov/publications/PubsSPs.html)

[p] NIST SP 800-57 Part 1 Recommendation for Key Management – Part 1: General (Revision 3), July 2012 (http://csrc.nist.gov/publications/PubsSPs.html)

[q] ENISA Algorithms, Key Sizes and Parameters Report - 2013 recommendations, version 1.0, October 2013 (https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report)

[r] Face Recognition Vendor Test (FRVT), Performance of Face Identification Algorithms, NIST Interagency Report 8009, May 2014 (http://biometrics.nist.gov/cs_links/face/frvt/frvt2013/NIST_8009.pdf)

[s] ISO/IEC 19795 (dates depend on the part) Biometric performance testing and reporting[1] (http://www.iso.org)

[t] International Civil Aviation Organization (ICAO) Doc 9303 (dates depend on the part) Machine Readable Travel Documents (http://www.icao.int/publications/pages/publication.aspx?docnum=9303)

[1] Please note that access to International Standards is on a subscription or payment basis.

Glossary

AC - Authentication and Credential

Authentication - The process by which a system confirms the user is known to that system, usually through the use of one or more Credentials

Authentication Provider - Provision of an Authentication service involves different stages, including Credential manufacture; Credential provision; management and revocation, and possibly others. Any particular solution could have a variety of different entities providing these services. Throughout this document this term will be used to refer to whichever of these services is relevant given the current context

Biometric - A measure of a human body characteristic that is captured, recorded and/or reproduced in compliance with ICAO Doc 9303 (reference [t]) or ISO/IEC 19794 (reference [s])

Credential - A set of identifiers, attributes and or information (which may be part of a token) with which a user proves their claim to an identity/account and enables authorised access to systems, information and services

Cryptographic Key - A sequence of numbers or characters that are used as input to a cryptographic algorithm

Entropy – Although there are many ways to define entropy, in this document it is used to indicate the predictability (or unpredictability, as a bigger entropy indicates more possibilities related to the chosen characters, numbers, etc.) of a value (e.g. the actual key value)

Factor - A way of classifying the types of Credentials the user can use. This is usually considered as one of the following: “something the user knows”; “something the user has”; or “something the user is”

IDP – Identity Provider

LTS – A Limited Time Secret is a Secret that is only valid within a short time period (e.g. a few minutes)

Multi-factor – An Authentication that requires more than one factor

OoB - Out of Band is a communication that occurs outside of the communication method/channel used for the Authentication

OTP - One Time Password, for the purposes of this document, is a computer generated Secret that is generated for the use in only one Authentication

PIN - Personal Identification Number

Secret - Information known only to the user which can be checked by the authentication system in support of an Authentication

TLS - Transport Layer Security (reference [h])

Token - A token is considered to be a hardware device, or piece of software running on a hardware device, that contains, or is linked to, a Credential that can be checked by the authentication system

IA
CESG
A2i
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Fax: +44 (0)1242 709193
Email: enquiries@cesg.gsi.gov.uk