The Road to Multilateral Recognition of Identity Assurance Programs

The Future of NIST Special Publication 800-63

Editor: KENNETH DAGG

Contributors:

Howard Staple — Identity & Information Assurance Advisor, Identity Assurance Programme, Government Digital Services, Cabinet Office

Alastair Treharne — Identity Assurance Advisor, Identity Assurance Programme, Government Digital Services, Cabinet Office

Paul Grassi — Senior Standards and Technology Advisor, National Institute of Standards and Technology (NIST), US Department of Commerce

Joni Brennan — Executive Director, Kantara Initiative

Abstract:

This study is one of a set of reports prepared by the Kantara Initiative to assess if it is viable for the United Kingdom (UK) Cabinet Office to recognize Identity Providers approved by other international bodies for use in the UK. The purpose of the series of studies is to determine the viability of multilateral recognition of national identity assurance programs. This report presents a discussion on potential evolution of the Electronic Authentication Guideline – Special Publication (SP) 800-63 of the National Institute of Standards and Technology (NIST).

Contents

1 PROJECT OVERVIEW

1.1 Project Purpose

This project is being undertaken by the Kantara Initiative to assess the processes currently being used by other international bodies to accredit and certify/approve Identity Providers (IDAs) with the goal of determining if it is viable for the United Kingdom (UK) Cabinet Office to recognize these IDAs for use in the UK. In other words, the purpose of the series of studies is to determine the viability of multilateral recognition of national identity assurance programs.

To test the feasibility of this approach of the UK Cabinet Office and start down the road to multilateral recognition, this project will provide a high level assessment of the processes used by the Federal Identity, Credential, and Access Management (FICAM) program of the Government of the United States of America (US) to accredit and approve IDAs for use by the US Government.

1.2 Project Objectives

Project Business Objectives

This project will specifically identify options, recommendations and timeframes based upon an:

- Assessment of the equivalence of Kantara Initiative's Identity Assurance Framework (IAF) requirements against the UK's requirements for Certification Bodies (CBs) and IDAs.
- Assessment of the equivalence of US Government and Cabinet Office requirements for CBs and IDAs including authentication governance.
- Assessment of the future direction and evolution of the National Institute of Standards and Technology (NIST) Electronic Authentication Guideline – Special Publication (SP) 800-63.

The options, recommendations and timeframes identified in this assessment will contribute to the Cabinet Office of the UK Government recognizing other jurisdictions as Accredited CBs that are able to certify IDAs to Cabinet Office standards, so that the Cabinet Office does not have to carry out the assessment of the IDAs. This in turn contributes to the Cabinet Office realizing its vision to create a market of certified, customer-focused services in the private sector that will provide a consistent way for customers to access any public service, and potentially private sector services.

2 CONTENTS

Section 3 of this document presents a brief history and overview of SP 800-63.

Section 4 presents the personal opinions of a NIST official as to how SP 800-63 should evolve.

Section 5 presents conclusions from the review of SP 800-63.

Appendix A contains a list of the Acronyms, Abbreviations and terms used in the document. Appendix B identifies the materials that were analyzed.

3 HISTORY AND OVERVIEW OF SPECIAL PUBLICATION 800-63

The NIST is the author and steward of SP 800-63 - Electronic Authentication Guideline. In addition to other specific organizational, privacy and operational requirements, the FICAM Trust Framework Solutions (TFS), Trust Framework Provider Adoption Process (TFPAP) For All Levels of Assurance requires compliance with the current version of NIST SP 800-63.

3.1 SP 800-63

The NIST released SP 800-63 - Electronic Authentication Guideline in April 2006 to supplement Office of Management and Budget (OMB) E-Authentication Guidance for Federal Agencies, [OMB 04-04].

It was released to provide technical guidance to support US Federal Government Agencies that wished to allow an individual person to remotely authenticate his/her identity to a Federal IT (Information Technology) system. It addressed only traditional, widely implemented methods for remote authentication based on secrets. With the methods it specified an agency could be assured that the individual to be authenticated knew or possessed some secret information.

The document identified appropriate technology that, at a minimum, met the technical requirements for the required level of assurance. In particular, the document stated specific technical requirements for each of the four levels of assurance in the following areas:

- Tokens – typically a cryptographic key or password, for proving identity
- Registration and Identity Proofing – the delivery of credentials which bind an identity to a token
- Authentication Protocols – that is the combination of credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be including assertion mechanisms used to communicate the results of a remote authentication to other parties

3.2 SP 800-63-1

SP 800-63-1 was released in December 2011 to supersede 800-63. The revision evolved and was reorganized to address:

- Tokens;
- Token and Credential Management;
- Authentication Processes; and
- Assertions.

3.3 SP 800-63-2

SP 800-63-2 was released in September 4, 2013 to supersede 800-63-1. The revision introduced substantive changes to the section that addressed Registration and Issuance Processes to facilitate the use of professional credentials in the identity proofing process, and to reduce the need to use postal mail to an address of record to issue credentials for level 3 remote registration. Like 800-63-1 it addressed:

- Tokens;
- Token and Credential Management;
- Authentication Process; and
- Assertions.

3.4 Request for Comments

In April 2015 NIST, in response to market innovation, evolving federal requirements, and an advanced threat landscape targeting remote authentication, issued a request for comments to identify areas that industry and government deem most significant for revision. The following developments were the impetus for the possible revision:

- Executive Order 13681 (Improving the Security of Consumer Financial Transactions) was issued by the administration in October 2014. This Executive Order required "…that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate."
- The roadmap accompanying the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) – published by NIST in February 2014 in response to Executive Order 13636 – cites the need for NIST to "…conduct identity and authentication research complemented by the production of NIST SPs that support improved authentication practices."
- The National Strategy for Trusted Identities in Cyberspace (NSTIC), released in 2011, charted a course for both public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions through an Identity Ecosystem. NSTIC called for the Federal Government to "lead by example and implement the Identity Ecosystem for the services it provides internally and externally." As the Identity Ecosystem starts to take shape, NIST guidelines should reflect and support it.

Though not limited to these topics, NIST specifically requested input on the following:

Future of NIST Special Publication 800-63

- Schemas for establishing identity assurance that have proven effective in providing an appropriate amount of security, privacy, usability, and trust based on the risk level of the online service or transaction.
- Whether identity assurance processes and technologies could be separated into distinct components.
- Innovative approaches to hardware available to increase confidence in remote identity proofing.
- The privacy considerations arising from identity assurance that should be included in a revision including specific privacy-enhancing technologies, requirements or architectures that should be considered.
- The requirements, processes, standards, or technologies that are currently excluded from 800-63-2 that should be considered for future inclusion?
- Whether a representation of the confidence level in attributes should be standardized in order to assist in making authorization decisions and what form should that representation should take.
- Methods that could be used to increase the trust or assurance level (sometimes referred to as “trust elevation”) of an authenticated identity during a transaction.

4 INTERVIEW WITH NIST OFFICIAL

During an interview with an official from the NIST office the following personal opinions were expressed concerning how SP 800-63 should evolve:

- The review of 800-63 should:
  - make it easier for organizations to determine that they are compliant. That is, to make compliance less interpretive and more specific;
  - modernize the technical guidance that it provides including:
    - use of biometrics;
    - remote proofing;
    - separation of proofing and authentication; and
    - dropping knowledge based tokens.
  - collapse and simplify the document to make it more readable and easier to understand; and
  - make requirements outcome based rather than prescriptive to allow changes to technology to be accommodated without having to release a new version.
- NIST is open to dropping Level of Assurance (LOA) 2 in order to comply with the recent Executive Order 13681 to use two-factor authentication whenever personal data is involved.

The scope of SP 800-63 would remain the US Federal Government. However, NIST would not forbid the private sector from adopting it if they so desired.

The opinions were expressed with the caveat that responses to the request for comments would be the ultimate factor in deciding how SP 800-63 would change.

5 CONCLUSIONS

The evolution of SP 800-63 is a seminal event because many other jurisdictions have based their specific requirements on this document. This being said, NIST expects, unless there is over whelming resistance, to significantly revise the requirements established by SP 800-63. In addition to making the document easier to read, these changes could include evolving 1) from a four level to a three level assurance model, 2) introducing new mechanisms such as biometrics, and 3) make it easier for organizations to determine that they are compliant.

These changes could affect the ability of the FICAM TFS TFPAP, which is based upon the current release of SP 800-63, to be aligned with Good Practice Guide (GPG) 43.

Further analysis will be required, upon release of the new version of 800-63, to ascertain the impact on GPG 43.

6 APPENDIX A – ACRONYMS, ABBREVIATIONS AND GLOSSARY

This appendix expands acronyms and abbreviations used in the project.

Term	**Definition**
CB	Certification Body
CESG	Communications-Electronics Security Group
FICAM	Federal Identity, Credential, and Access Management
GPG	Good Practice Guide
IAF	Identity Assurance Framework
IDA	Identity Assurance Provider
IT	Information Technology
LOA	Level of Assurance
NIST	National Institute of Standards and Technology
NSTIC	National Strategy for Trusted Identities in Cyberspace
OMB	Office of Management and Budget
SP	Special Publication
TFPAP	Trust Framework Provider Adoption Process
TFS	Trust Framework Solutions
UK	United Kingdom
US	United States of America

7 APPENDIX B – ANALYSIS REFERENCE MATERIAL

- Good Practice Guide 43 - Requirements for Secure Delivery of Online Public Services, Issue No: 1.1, December 2012, Communications-Electronics Security Group (CESG), Crown copyright 2012.
- E-Authentication Guidance for Federal Agencies, Office of Management and Budget (OMB) M-04-04, December 16, 2003
- Electronic Authentication Guideline, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-2, Version 2, August 2013
- Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS), Trust Framework Provider Adoption Process (TFPAP) For All Levels of Assurance, Version 2.0.2, March 14, 2014

8 REVISION HISTORY

0.1 May 10, 2015 Initial Draft

1.0 May 31, 2015 Final