

Post-quantum authentication for digital identity services in the cloud

IAB Workshop on Accelerating the Deployment of Post-Quantum Authentication

Francis Lewis (francis.lewis@dsit.gov.uk) & Jess Winterborne (jess.winterborne@dsit.gov.uk)

Government Digital Service, Department for Science, Innovation and Technology

Introduction

GOV.UK One Login is the central authentication and identity proofing system used by over 200 public-facing government services in the UK. It supports tens of millions of users and makes heavy use of cryptography within a serverless architecture running on AWS. Authentication is implemented across many layers, including internal and external OAuth interfaces and verifiable credentials (VCs), both of which are secured using JOSE. Given the central role it plays in providing citizens with access to a broad range of government services, a smooth migration to post-quantum authentication is necessary to maintain the required level of security and trust in the system.

PQC at GOV.UK One Login

Early-stage activities to support PQC migration are underway. Alongside a cryptographic inventory, PQC trials have been carried out in a sandbox environment, with some limited production deployment. Our main findings come from a minimal implementation of core identity proofing and verification services, used to explore potential technical impacts and support migration planning. The primary focus of these activities was to understand the state of current implementations, transport constraints when using OAuth flows within a serverless architecture on AWS, and the coordination challenges migration involves.

Findings and open challenges

Transport constraints within AWS when using OAuth 2.0

JWT-Secured Authorization Requests provide a way to protect OAuth 'authorize' request parameters via signing and optional encryption. When passed by value, these objects are transmitted as base64url encoded strings within URL query parameters, meaning URL length increases significantly when using PQ signatures like ML-DSA.

Within AWS, there are multiple components with URL size limits such as API Gateway (8/10 KiB), CloudFront (8 KiB), and Application Load Balancer (16 KiB for request line). Firewalls are often configured with even lower limits, and are therefore likely to encounter issues first. Pushed Authorization Requests and other pass-by-reference techniques are supported by OAuth and recommended by high-security OAuth profiles such as FAPI. These approaches alleviate URL size constraints and can improve cryptographic agility, but also introduce additional security considerations and migration challenges.

Where multiple cryptographic operations are required for a single user journey, the overall data transfer also increases significantly, resulting in much higher network ingress/egress. For a typical identity proofing and verification journey including both authentication and key establishment, we saw the cumulative network egress increase from 6.7 KB to 44.5 KB for PQ-only (ML-DSA-65 + ML-KEM-768), and to 56.7 KB for PQ/T (X-Wing + ML-DSA-65/ES256).

Phased migration and dual-running schemes

PQC migration is expected to take place in phases, with a period in which traditional and PQ algorithms run in parallel. GOV.UK One Login interacts with a large number of other government departments through a single public interface and associated key set, and we should expect migration timelines to vary between these organisations. Dual-running will also enable a controlled rollout of PQC to a subset of traffic while it is being tested. Similar challenges apply to internal interfaces which will require a significant engineering effort to migrate, however coordination should be more straightforward than for migrations involving external organisations.

JSON Web Key Sets are used for public OAuth keys, and decentralized identifier documents are used for VC keys. Both formats support multiple keys, and this is currently used to support several algorithms and key rotations. PQ/T introduces further challenges, including avoiding cross-protocol key reuse between traditional and PQ/T schemes. Downgrade attacks, such as signature stripping, and other PQ/T-specific migration risks must also be addressed.

Re-signing existing credentials

Millions of internal VCs will also need to be re-signed safely with zero downtime. Similar to OAuth interfaces, multiple algorithms will have to be supported simultaneously during migration, but there are additional concerns around credential semantics such as re-signing versus re-issuing credentials, credential status, and verifier compatibility.

Library implementations

Within high-level libraries, support for PQ signature algorithms is generally more mature than for PQ KEM algorithms, although production-ready ‘out-of-the-box’ support is still limited. When using JOSE, popular libraries often do not support features until they are included in the relevant standards. As a result, assessing the impact of anticipated features (such as PQC algorithms and composite signatures) currently requires custom test implementations. Of the libraries and services we tested that support ML-DSA for PQ authentication, we have not found signing or verification latency to be a problem. Our benchmarking of AWS KMS shows that while on average ML-DSA-87 signing is roughly 50% slower than ES256, the absolute difference remains small (approximately 6 ms versus 9 ms).

Lack of clarity around PQ/T guidance

Hybrid PQ/T schemes are appealing as a transitional measure, however there is a lack of concrete guidance on how best to deploy them. Both NIST and the UK’s NCSC allow for the use of PQ/T in appropriate circumstances, but offer much less practical guidance than is available for PQ-only algorithm selection. For example, open questions remain around the trade-offs between composite and dual signature models within JOSE, OAuth, and VCs. The level of additional scrutiny required for PQ/T schemes, beyond that needed for PQ-only deployments, is also unclear. Further security analysis is likely necessary, but it remains uncertain how responsibility for this will be divided between standards bodies, library implementers, and consuming organisations.

Conclusion

Our experience suggests that the main barriers to PQ authentication are protocol transport constraints, ecosystem coordination, and the lack of clear deployment patterns for phased and hybrid migration.