Arqit Quantum Inc.

Growing acceptance of Arqit cloud-based services

5 March 2024

Accelerating take-up and collaboration

Arqit has developed secure encryption based on the cloud-based agreement of pairs of symmetric keys at end points, a solution to the limitations and frailties of Public Key Infrastructure (PKI), the basis of current encryption processes. Having successfully demonstrated secure key agreement across cloud-based facilities and a wide range of OEM applications, Arqit has now recorded a number of adoptions of its *Symmetric Key Agreement Platform* (SKAP) amongst telecoms service providers and in the financial services sector.

Arqit's current positioning and the increasing interest it is reporting from vendors, partners and distributors can be traced to it having declared compliance with the NSA Commercial Solutions for the Classified Symmetric Key Management Requirements Annex 2.1 encryption standard. NIAP, the National Information Alliance Partnership, has also mandated the adoption of *RFC8784* - which describes the use of symmetric keys - within the Standard for VPNs operating under NSA's Commercial Solutions for Classified (CSfC) programme, and to which Arqit's SKA is fully compliant. Arqit has partnered with major OEMs in the USA such as Fortinet, HPE and Juniper who have validated and recognised the significance of this compliance.

The importance of the NSA

The NSA sits at the heart of US security interests and has far-reaching influence. Arqit's NSA-compliant solution places it ahead of other post-quantum cryptography algorithms which are yet to be standardised. In our view, its SKAP has become the **'gold standard'** for network encryption and materially raised Arqit's profile within the cybersecurity and communications community. During FY23, the Group launched two principal SKAP applications for target verticals: **Arqit NetworkSecure™** for network firewalls, and **Arqit TradeSecure™** for digitised trade finance documents, and has secured OEM integration partnerships with Fortinet, Juniper Networks and Hewlett Packard, in addition to distribution agreements with BT, Babcock, Dell and others. On 5 March 2024 Arqit added a reseller agreement with Total Computers for SKAP and NetworkSecure™ Adaptor.

FY23 earnings update

For the year to 30 September 2023, Arqit reported QuantumCloud™ revenue of US$0.69m from 7 contracts, with US$4.96m from discontinued operations (FY22: US$7.21m and US$12.84m from discontinued operations). Market demand for data encryption and network and data security continues to grow, having reached US$169bn by 2022 (Gartner Group: https://www.gartner.com/en/documents/4019160), and estimated to be US$262bn by 2026 (2019-26 CAGR: 12.3%). In addition to the value of data flows requiring protection, the rapidly approaching reality of viable quantum-based decryption emphasises the need to replace the vulnerable PKI-based systems which currently underpin this market.

Sector valuation: implications

Current EV/EBITDA valuations in the cybersecurity sector indicate a market cap-weighted average of 55.5x, median 35.4x, and EV/Revenue (market cap weighted) of 13.0x. Cross-referenced to sector market valuations, in order to address the question of valuation, we suggest a *hypothetical* future benchmark Arqit revenue base of US$100m which, if achieved, would cross-refence with market EV/Revenue to **indicate an equity Fair Value of US$9.2 per share.**

Company Data

NASDAQ quote	ARQQ
Share price (last close)	$0.78
Market cap	$126m
ED Fair Value / share	$9.2

Share Price, US$

Source: ADVFN

Description

Arqit Quantum Inc. is an innovative developer and provider of post quantum cryptographic software service which delivers rotating authentication and encryption that is held to be quantum safe.

Arqit has turned deep tech into a platform-as-a-service offering which is software-light and highly scalable, with worldwide distribution capability.

Its online sales model targets a wide range of verticals, initially in the defence, telecommunications, autonomous vehicles, and financial services sectors.

Arqit has assembled a management team with depth in technology and contacts with top-level decision takers in leading companies and government bodies.

Mike Jeremy (Analyst)
0044 207 065 2690
mike.jeremy@equitydevelopment.co.uk

Andy Edmond
0044 207 065 2691
andy@equitydevelopment.co.uk

FY23 performance

Having launched Arqit QuantumCloud™ in H2 22, Arqit reported QuantumCloud™ FY23 revenue of US$0.69m, with US$4.96m from discontinued operations, compared to US$7.21m (US$4.7m from an enterprise licence to Virgin Orbit) and US$12.84m from discontinued operations (of which US$ 5.0m was from the European Space Agency) in FY22. QuantumCloud™ revenue comprised 7 contracts. As shown below:

- Operating costs decreased 22%YoY, from US$72.15m to US$55.20m; adjusted for non-cash share-based payments, US$41.08m reduced from US$49.24m (-16.6%YoY) in FY22.
- Capital spend was minimal, at US$0.71m, compared to US$2.38m in FY22.
- The year-end cash position was US$44.46m, a US$4.5m reduction from FY22 (US$48.97m).

Summary financial data FY20 – FY23

Year to 30 Sep, US$m	2020	2021	2022	2023
Revenue	**1.964**	**0.048**	**7.212**	**0.693**
Sum Operating Costs	(2.773)	(14.559)	(70.977)	(55.201)
Reverse acquisition expense	0.000	(155.460)	0.000	0.000
Listing	0.000	(2.590)	0.000	0.000
EBIT Reported	(0.809)	(172.561)	(63.765)	(84.444)
EBIT Adjusted	**(0.687)**	**(172.396)**	**(42.023)**	**(70.326)**
EBITDA Reported	(0.804)	(172.508)	(62.473)	(83.152)
EBITDA Adjusted	**(0.682)**	**(172.343)**	**(40.731)**	**(69.034)**
PBT Reported	(1.137)	(271.729)	53.408	(74.049)
PBT Adjusted	**(1.015)**	**(173.474)**	**75.150**	**(59.931)**
PAT Reported	(0.515)	(271.344)	68.176	(71.960)
PAT Adjusted	**(0.393)**	**(173.089)**	**89.918**	**(57.842)**
Basic wtd. av. shares (m)	59.261	68.326	121.161	131.469
EPS rptd basic ($c)	**(0.959)**	**(397.692)**	**53.709**	**(56.217)**
EPS reptd diluted ($c)	(0.959)	(397.692)	48.491	(51.145)
EPS adj basic ($c)	(0.753)	(253.890)	71.654	(42.805)
EPS adj diluted ($c)	(0.753)	(253.890)	64.692	(38.943)
Cash from operations	(2.140)	(24.304)	(41.427)	(21.140)
Net cash from operations	(1.334)	(24.035)	(26.719)	(32.784)
Net cash used in investing	(4.571)	(9.305)	(24.432)	(16.123)
Net OpFCF	(5.905)	(33.340)	(51.151)	(48.907)
Net cash from financing	1.680	120.105	22.176	44.853
Forex	0.193	0.006	(9.025)	(0.457)
Cash at year end	0.195	86.966	48.966	44.455
Sum Fixed Assets	8.836	23.468	67.229	13.436
Sum Current Assets	0.475	90.258	56.643	86.349
Sum Current Liabilities	(7.846)	(17.069)	(23.809)	(26.818)
Sum Long-term liabilities	(0.534)	(130.498)	(21.508)	(6.314)
Retained earnings	(0.486)	(272.215)	(207.140)	(277.533)
Equity	0.930	(33.840)	78.555	66.653

Source: Company data. Form 20F. Equity Development estimates (adjusted data).

Cryptography progresses: from PKI to RFC 8784

A reminder of the frailties of conventional encryption

As we have noted (Equity Development report 18 July 2021: Unbreakable quantum encryption: the 'holy grail') the most widely-used means of data encryption (and basis for security in areas such as HTTP-based TLS/SSL, Transport Layer Security / Secure Sockets Layer, internet communication) is Public Key Infrastructure (PKI). In PKI encryption the public key is 'open' to all and encodes the message, whilst the private key is not revealed and decodes the message. The addition of a PKI certificate establishes the identity of the sender in the message exchange process, which must also be referenced by a trusted source or certificate authority (CA). This approach relies on (i) ***trust*** in the validity and security of its public and private keys and certificates, and (ii) ***mathematical*** reliance on deciphering long strings of prime numbers which it is assumed conventional computing is unable to solve in a time-effective manner (see: https://www.okta.com/identity-101/public-key-infrastructure).

PKI 'trust' has been compromised. PKI has a long history of failures resulting from weak implementation, ranging from certificate-based failures (e.g. Verisign Microsoft certificates, Superfish Addition of Root Certificates, or Marlinspike Certificate Constraint Omission), application layer failures in areas such as TLS Protocol and Weak Hash Functions, or poor implementation. The 'mathematical' basis of PKI encryption is also increasingly vulnerable as the advent of quantum computing introduces the possibility of real-time computational code breaking (see IBM 2023 'bringing useful quantum computing to the world' https://www.ibm.com/quantum). The reality of this future is evident in the growing practice of intercepting and storing potentially useful encrypted data for *future* quantum-based decoding: "store-now, decrypt-later". Fundamentally PKI is vulnerable as:

- "*A future attacker is able to use quantum computing to break the public-key encryption and breach the security of the locking systems by obtaining access to the private key of a root certification authority. The attacker can then use this key to create signed certificates at its convenience*". KPMG *Market Survey on Cryptography and Quantum Computing,* 2023.

Shor's algorithm and Mosca's theorem

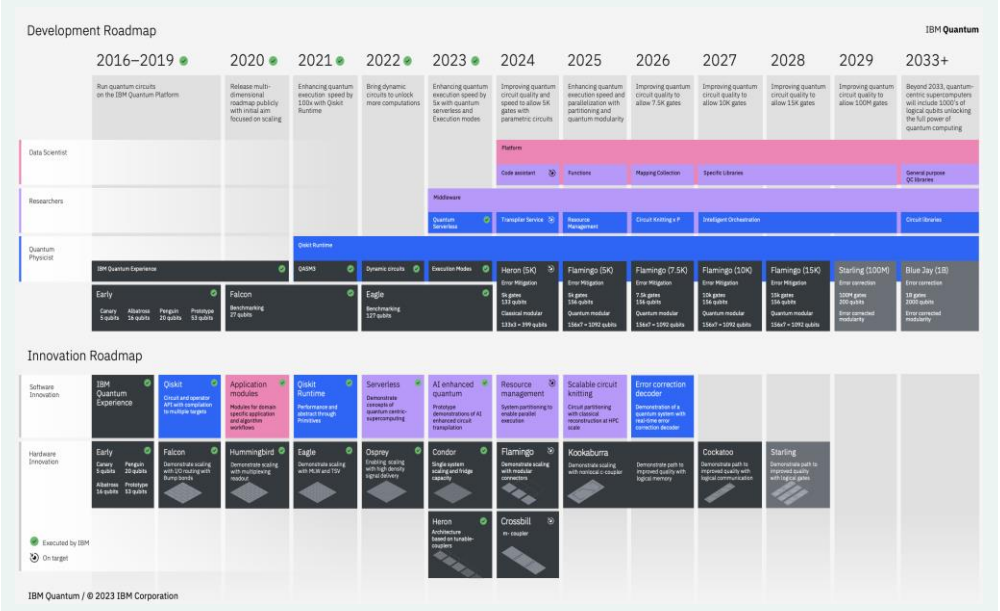
In 1994 MIT Professor of Applied Mathematics Peter Shor devised 'Shor's algorithm' which demonstrates how to resolve the large-number factor used in cryptography, the only problem being that this was beyond – and remains beyond – the power of the current generation of digital computers. However, quantum computing makes Shor's algorithm a reality.

The theoretical physicist Michele Mosca succinctly summarised the time frame left to develop quantum computing-resistant cryptography in a formula: (i) x is the number of years for which the data needs to be secured, (ii) y is the number of years required to develop quantum computing-resistant cryptography, (iii) z is the number of years left before quantum computers can break current cryptography. If $[y+x] > z$ then current PKI-based cryptography will have been rendered ineffective without a viable alternative in place. Mindful of the urgency created by advances in quantum computing this continues to spur interest in alternatives to PKI-based encryption.

Quantum computing continues to develop

IBM provides an example of the interest in and pace of quantum computing development. As illustrated below in its *Development Roadmap*, IBM's latest quantum computing iteration is the 133-qubit* *Heron* succeeding '*IBM Eagle*' with 127qb. Following demonstration of the concept processor '*Condor*' at 1,121qb, IBM targets '*Flamingo*' at 1,386+qb and '*Kookaburra*' at 4,158+qb by 2026. In addition, IBM's 'System 2' quantum computer architecture is designed to accommodate add-on units, enabling an estimated 16,632qb. (*for a description of qubits see https://azure.microsoft.com/en-gb/resources/cloud-computing-dictionary/what-is-a-qubit).

IBM Quantum - development roadmap 2023



Source: https://www.ibm.com/quantum/summit-2023.

As reported in the Financial Times on 5 January 2023 there are claims that Chinese researchers have achieved decryption using quantum computing: "Computer security experts were struggling this week to assess a startling claim by Chinese researchers that they have found a way to break the most common form of online encryption using the current generation of quantum computers, years before the technology was expected to pose a threat. The method, outlined in a scientific paper published in late December, could be used to break the RSA[1] algorithm that underpins most online encryption, using a quantum machine with only 372 qubits." ([1] Rivest-Shamir-Adleman public key).

With this in mind there is evidence that alternatives to PKI are receiving serious attention.

Addressing the post-quantum world: accepting symmetric keys

Cyber security agencies, national-level security agencies and enterprises now accept that the threat of quantum computer-based decryption requires new strategies for data protection. These generally devolve into two groups: **post-quantum algorithms** (PQAs) and/or the adoption **of symmetric keys** to replace 'trust-based' PKI. In this respect, **we note the shift in cryptographic stance adopted by the US National Security Agency (NSA) in its Commercial Solutions for Classified programme which emphasises the role of symmetric keys**.

The adoption of a standardised PQA faces two persistent problems; (i) early evidence of fallibility, and (ii) (mindful of Mosca's theorem) often a long timeframe required for exhaustive tests. There are recent examples PQA failures even after successive rounds of tests and simulated attacks:

- **March 2022: Rainbow,** *multivariate signature scheme*: "One of three cryptography algorithms vying to become a global standard against the looming security threat posed by quantum computers has been cracked in a weekend using a standard laptop": New Scientist, "Encryption meant to protect against quantum hackers is easily cracked", 8 March 2022 which can be accessed here: (https://www.newscientist.com/article/2310369-encryption-meant-to-protect-against-quantum-hackers-is-easily-cracked). Also reported by Cryptomathic: https://www.cryptomathic.com/news-events/blog/nist-pqc-finalists-update-its-over-for-the-rainbow).

- **August 2022: Supersingular Isogeny Key Encapsulation - SIKE:** "one of the four encryption algorithms America's National Institute of Standards and Technology (NIST) considered as likely to resist decryption by quantum computers has had holes kicked in it by researchers using a single core of a regular Intel Xeon CPU, released in 2013": The Register, Post-quantum crypto cracked in an hour with one core of an ancient Xeon, 3 August 2022.

  See: https://www.theregister.com/2022/08/03/nist_quantum_resistant_crypto_cracked.

Symmetric keys gain traction

By contrast, a number of recent announcements indicate the growing traction of symmetric key protection:

- **4 May 2022**: the White House mandated the use of symmetric encryption stating that agencies maintaining National Security Systems *"shall implement symmetric-key protections"* to provide additional protection for quantum-vulnerable key exchanges: National Security Memorandum NSM-10: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems

- **7 September 2022:** the **National Security Agency (NSA)** has stated that they consider the use of pre-shared symmetric keys *"in a standards-compliant fashion a better near-term post-quantum solution than implementing experimental post-quantum asymmetric algorithms"*: NSA Commercial National Security Algorithm Suite 2.0 https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

- **2 October 2023**: Arqit itself declared that its SKA is a commercial solution that meets the demands of US National Security Memorandum 10 and CSfC Symmetric Key Management Requirements Annex 2.1. Whilst we expect that Arqit is constrained in describing interaction with cyber agencies and related bodies, Arqit's statement has veracity.

- **23 August 2023: Germany's Federal Office for Information Security (BSI)** warned that organisations expect to complete the migration to quantum-safe cryptography *"6.5 years too late*" and that *"if confidential information can be read for many years, possibly while going unnoticed, this could have serious consequences."* KPMG Market Survey on Cryptography and Quantum Computing for the Federal Office for Information Security. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Marktumfrage_EN_Kryptografie_Quantencomputing.pdf?__blob=publicationFile&v=3

- **20 December 2023:** the **French Cybersecurity Agency (ANSSI)** stated that PQAs are not viewed as *"mature enough to solely ensure the security"* and recommend hybrid protocols in the short- and medium-term, with pre-shared keys an alternative valid solution. (https://cyber.gouv.fr/en).

- **January 2024: France, Germany, The Netherlands, and Sweden** collectively called for *"the migration to post-quantum cryptography in hybrid solutions with traditional symmetric keying or classically secure public-key cryptography." 26.01.2024* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html

Symmetric keys become a commercial standard: *RFC 8784*

WiFi is now almost ubiquitous in wireless connectivity across enterprises and into the home. Its origins lie in a set of standards which were adopted and finalised in 1997 by the Institute of Electrical and Electronic Engineers (IEEE) LAN/MAN Standards Committee, known as IEEE 802.11. This arcane acronym is the widely used platform on which almost all local WiFi networks now interact with the ethernet.

RFC 8784 represents the establishment of an encryption protocol of similar significance to 802.11. Through its National Information Assurance Partnership (NIAP) programme, in August 2023 the NSA stipulated that virtual private network (VPN) gateways (a router or switch) used in classified solutions **must be *RFC 8784-compliant***. (https://www.niap-ccevs.org/MMO/PP/MOD_VPNGW_v1.3.pdf). Just as the IEEE established the WiFi protocols embedded in 802.11, the Internet Engineering Task Force (IETF) determined how symmetric keys could be used to render Shor's algorithm irrelevant and guarantee that networks could not be compromised: RFC 8784 (see Appendix I).

RFC 8784 establishes a protocol for mixing pre-shared keys to establish post-quantum computing security, set out by the NSA as 'Commercial Solutions for Classified (CSfC). https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/capability-packages/Key%20Management%20Requirements%20Annex%20v2_1.pdf

In summary, RFC 8784 effectively states that the NSA has concluded that symmetric key agreement meets the requirements to address post quantum-computing decryption by placing communications beyond the reach of interception and mathematical solution. At the same time the NSA indicated that this should be the *de facto* means of protecting commercial networks (VPNs). One consequence is that it also establishes Arqit's position as a leading developer and provider of symmetric key encryption.

Arqit Symmetric Key Agreement Platform (SKAP)

Arqit's Symmetric Key Agreement Platform (SKAP) enables two (or more) endpoints to 'agree' symmetric keys on demand, matching the requirements published by CSfC (see: Arqit Symmetric Key Agreement for Quantum-Safe Security of Classified Solutions, 2 October 2023 https://arqit.uk/resources/arqit-symmetric-key-agreement-for-quantum-safe-security-of-classified-solutions).

Arqit SKAP is currently also the only RFC 8784-compliant, and *quantum safe* cloud-based software method of agreeing symmetric keys, the main alternative being via a physical hardware device, with obvious drawbacks for security, and limitations on distribution at distance and scale.

In contrast to PKI, the approach developed by Arqit is **'split-trust'** i.e. it removes the requirement of public key 'trust' in an authentic 'private' key. This arrangement is replaced by a pair of identical keys which are symmetrical, are created simultaneously and contain matching long random numbers which cannot be reverse engineered.

However, in developing SKAP Arqit faced **the problem of how to distribute the key pairs**. Having initially considered a satellite-based system of distribution, Arqit refined its offering for cloud-based key agreement method with the following attributes:

- The creation and secure storage of random numbers in globally distributed data centres. Keys sourced from data centres hosting Arqit QuantumCloud™ to which replicated entropy is distributed (via classical digital hardware and software).
- Introducing a 'tumbler' in the form of 'rotating authentication'; key strings are refreshed as frequently as required. Rather than being vulnerable to break-in, digital or otherwise, the fact that keys change frequently eliminates the possibility of interception.

- Installation of a software agent to enable two or more devices to create a new symmetric key at the precise moment required; there is no point of interception available, and keys can be created for any size of group and refreshed as required. End point security – 'distributed secure communications cryptography' (DSCC) – creates symmetric key-protected channels, group or session keys. Crucially, the keys are 'self-creating'. This is the basis for (i) limitless key creation, and (ii) mass market access.

Additional features of benefit to network security

Arqit has been able to demonstrate that its keys are intrinsically 'quantum safe'. However, the architecture of Arqit's solution has two additional features, unconnected to quantum properties, which are of benefit to network security: distribution of certificates and anti-spoofing authentication.

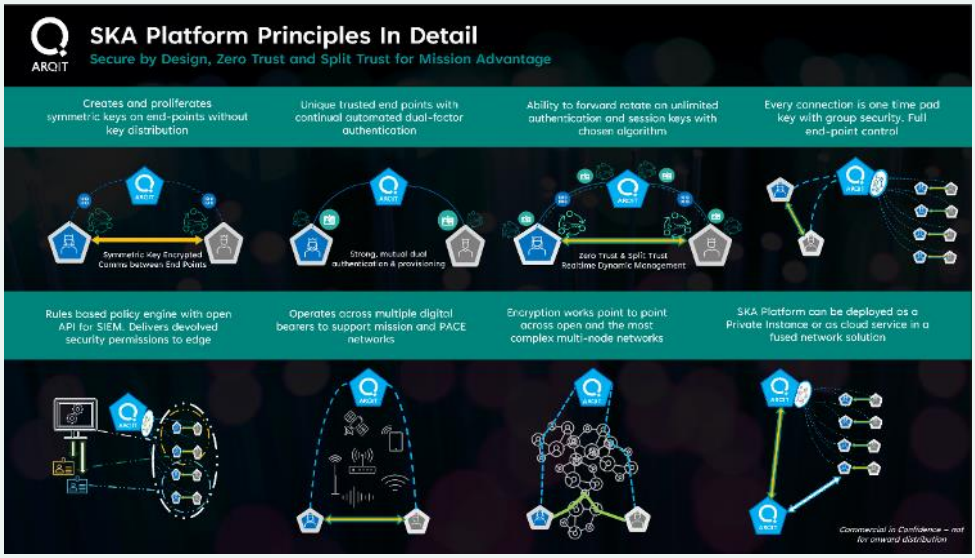
Certificates. PKI and its PQS successors require certificates provided by third parties to generate the initial root of trust. Certificates have been compromised in a number of high-profile attacks, and often they expire (e.g. the display "Certificate Not Trusted" appears on a public WiFi service indicates that the vendor has omitted to renew a certificate, or that the service has been compromised). Moreover, the proliferation of devices, especially with the advent of IoT sensors, means that attaching a certificate to every device is simply not viable. Arqit's SKA does not require third party certificates and is 'small' enough to run even on micro devices, of benefit to the security of proliferating devices with the growth of IoT and 5G connectivity.

Authentication and Spoofing. Currently a mal-actor can sniff a key by scouring traffic (especially on open wireless networks) being used by a device in order to authenticate onto a network and later use this identity to impersonate the device, i.e. "spoof" onto the network. With Arqit's SKA, the authentication key rotates by policy set by the user, as frequently as every second, rendering any key used in the past ineffective.

Interoperability and commercialisation

It is important that Arqit's resulting (Arqit 2022 Form 20F p 26) SKAP is available as a " 'Platform as a Service' (PaaS) that effectively creates a secure global mesh between different cloud providers and on-premises data centres around the globe." The fact that SKAP has to interpolate different network protocols means that it acts as an instantaneous network integrator as communications from one system are automatically encrypted for transmission and decryption by another. Arqit reports its technology currently has over 1,966 patent claims on 41 pending or granted patents in the UK, plus filings in other jurisdictions.

Arqit SKA platform principles



Source: Company data: Standard Arqit Non-NDA Customer presentation.

Target verticals

Arqit has so far defined three SKAP applications defined by target verticals, and has secured partners for applications principally for network security and for financial transactions:

- **NetworkSecure™**: integration of SKAP with the network devices of vendors including Juniper Networks and Fortinet, providing quantum-safe end-to-end symmetric key encryption.
- **TradeSecure™**: to provide Digital Negotiable Instruments, including Promissory Notes and Bills of Exchange, compliant with the UK Trade Documents Act 2023.
- **WalletSecure™**: to provide digital asset security and compliance analytics to prevent any change in a transaction before it is locked into a blockchain ledger.

Arqit's SKAP application partnerships are summarised below:

Source: Arqit presentation January 23rd 2024.

A cyber security market opportunity worth US$262bn

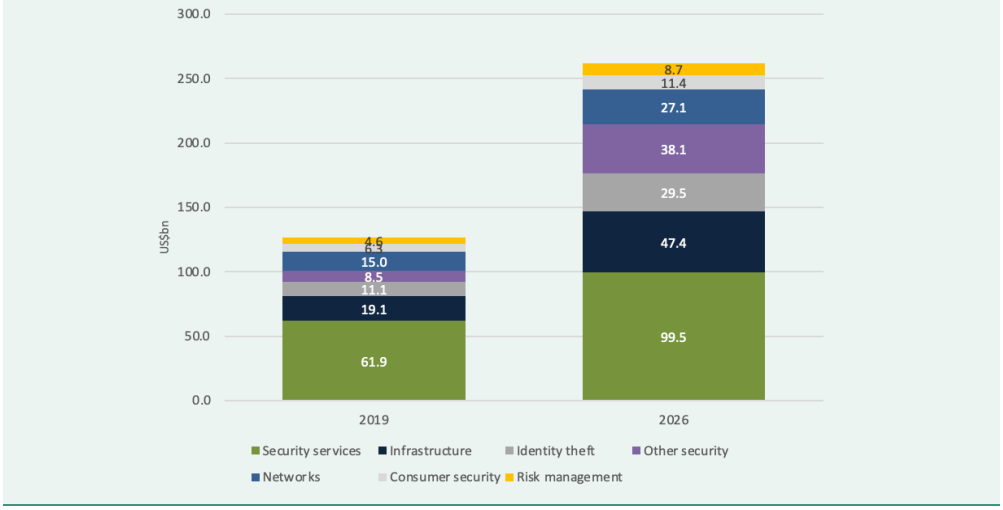
The global market for information security services is considerable, estimated by Gartner research to reach US$262bn by 2026, representing a CAGR of 10.9% from 2019 (US$127bn), and reached an estimated US$169bn by 2022 (https://www.gartner.com/en/documents/4019160).

As we have noted, the current standard means of encryption is Public Key Infrastructure, which if vulnerable to the expected arrival of quantum computer-based decryption, means a complete 'refresh' of encryption processes is required. Arqit's SKAP encryption solution is applicable to all areas and aspects of information security, i.e. all aspects of the market described.

The solution has gained traction in the areas of network security and financial transactions which share features which are intrinsic to a range of verticals:

- Defence-related communications and networks, infrastructure protection and data security, information sharing between security services.
- Large enterprise network security, cloud, data and consumer transaction authorisation.
- Financial services networks, applications, identity (validation and protection) and risk management.
- Telecommunications infrastructure provision, for emerging IoT networks, 5G deployments, ancillary key infrastructure protection (utilities, services and 'smart city' combined systems).

Information security services addressable market segments 2019, 2026



Source: Arqit, 2022 Form 20-F p24, based on Gartner, Inc. research. Gartner, Inc., Forecast: Information Security and Risk Management, Worldwide, 2019-2026, 3Q22 Update, September 28, 2022.

Arqit FY22–24: milestones

During FY22-24 Arqit announced a number of milestone collaborations, contracts and initiatives spanning a wide range of projects and geographies that included: UK 5G network, IoT and autonomous vehicles secure communications development; security for the major Saudi NEOM project; Asia-Pacific quantum key encryption development and deployment; military collaborations with the UK MOD and USAF; and UK government-level secure communications development. In chronological order these are:

Agreement with Juniper Networks

11 September 2021: Technology Alliance Partner Connect agreement with Juniper Networks to develop quantum-resistant network security using quantum encryption.

Autonomous systems - Blue Bear Systems Research

21 October 2021: agreement with the developer of unmanned and autonomous systems, Blue Bear Systems Research Ltd. (see https://bbsr.co.uk).

Saudi mega-project - NEOM *cognitive city*

8 December 2021: memorandum of understanding (MoU) agreement with NEOM ('New Enterprise Operating Model') Tech Digital Company (https://www.neom.com/en-us/sectors/technology-and-digital), and affiliate NEOM Company, to build and trial a 'Cognitive City' quantum-based security system. The project will develop cyber defences for NEOM, the 'world's first cognitive city', located in the Tabuk region of north-west Saudi Arabia.

Partnership with AUCloud

18 January 2022: addition of Sovereign Cloud Australia Pty Ltd - AUCloud - to the FQS participation, in partnership with the Australian Government. AUCloud is designed to provide high security sovereign cloud services to the Australian Government, Defence, Intelligence, and Critical National Industry (CNI) communities on an Infrastructure-as-a-Service (IaaS) basis, and is backed by the strategic investor NextDC (see: https://www.nextdc.com/). Initial projects include defining technical contributions, establishing the industrial supply chain, and preparing to deploy Arqit QuantumCloud™.

UK 5G cellular platform security selection

26 January 2022: selection by the UK Department for Digital, Culture, Media and Sports (DCMS) to develop a wideband solution for next generation 5G wireless Open Radio Access Networks (RAN) platforms, specifically to develop default security systems in order to secure any network device against attack, including quantum computer based.

USAF cooperative R&D agreement (CRADA)

4 February 2022: CRADA signed with the USAF Research Laboratory, Directed Energy Directorate, Space Electro-Optics Division to demonstrate interoperability and performance of QuantumCloud™ in defence scenarios. The trials include USAF-DoD communications systems.

Next generation communications – UK MOD contract

12 April 2022: a contract to join the UK MOD's Framework for Connectivity of Disparate Remote Autonomous Systems - 'MDIS', Multi-Domain Integrated Systems project. MDIS is tasked with developing common standards and architectures for interfaces, data transfer and data management spanning legacy communications systems and upgrades.

Independent assurance reports prove "excellence"

11 May 2022: independent assurance review of Arqit's technology and reports by the University of Surrey ('Tamarin Prover') and PA Consulting. The University of Surrey subjected Arqit's solution to 'Tamarin' scrutiny - "the industry preferred tool" for verifying the robustness of a cryptographic protocol - to which its ascribed "excellent" performance.

PA Consulting applied the Tamarin Proof to the Arqit Protocol Framework and reached the same conclusion: "The findings give us confidence the core protocols defining the building block for security of computing device-to-Cloud connectivity will meet their stated security goals". On 9 May at CYBERUK 2022, Arqit successfully demonstrated integration of QuantumCloudTM into cybersecurity specialist Fortinet's architecture, resulting in an effective quantum-secure firewall.

Industrial IoT comms security

11 May 2022: with Blue Mesh Solutions Limited (see: https://bluemeshsolutions.com), a UK-based sensors and Internet-of-Things specialist, successful demonstration of 'quantum-secure MQ Telemetry Transport' within the UK Government's DCMS 5G *Trials and Testbeds* programme.

Availability of AUCloud quantum encryption

9 October 2022: AUCloud launched the first Quantum Safe Symmetric Key Agreement Software (SKAS), provided by Arqit QuantumCloud™, available as a platform-as-a-service, offering protection against the practice of data gathering for subsequent decryption ('harvest now, decrypt later') in areas such as government and defence communications, IoT transmission or commercial transactions.

Secure UK government gateways - Nine23 encryption partnership

25 October 2022: partnership with cyber security specialist Nine23 (https://www.nine23.co.uk) to provide cyber security solutions for UK regulated and compliant sectors using Arqit QuantumCloud™, on Nine23's UK Sovereign Secure Private Cloud infrastructure (*Platform FLEX*).

The Nine23 platform is used secure direct gateway connectivity to UK government networks suitable for Official Sensitive high-security classified data and communications. Launch was set for 9th November.

QuantumCloud™ powered by AWS

9 December 2022: application of Arqit's QuantumCloud™ on Amazon Simple Storage Service (Amazon S3) – a scalable object storage service, currently containing over 200 trillion objects with an average 100m requests per second - powered by Amazon Web Services (AWS).

Traxpay contract

12 December 2022: contract with Traxpay GmbH (www.traxpay.com), the Frankfurt-based supply chain finance specialists, to deliver quantum-secured digital finance instruments based on Arqit's *TradeSecure* distributed ledger technology. Traxpay is customer of Arqit using QuantumCloud™ via AWS. The system will provide Traxpay customers with a referenceable digital finance Promissory Note or Bill of Exchange backed by Arqit's QuantumCloud™ quantum-safe security. The combination of Arqit's provable data original certification and QuantumCloud™ offers the required protection as this digital documentation market develops.

Partnership with Dell

13 December 2022: signed a 'Dell OEM Engineered Solutions Pilot Agreement' with Dell Technologies, under which Dell agrees to preload Arqit's QuantumCloud™ software on selected Dell devices for sale as a combined hardware-software SKU. The collaboration targets the US Federal Government: Department of Defense, Federal Civilian Agencies, and Intelligence Community. In particular, this is aimed at counteracting the 'harvest now, decrypt later' practice.

Fortinet Fabric-Ready Partner Programme

14 December 2022: joined the Fortinet Fabric-ready Partner Programme as a Technology Alliance Partner enabling integration of Arqit QuantumCloud™ with Fortinet's FortiGate Firewalls solution.

DETSAD strategic agreement

12 June 2023: strategic agreement to develop security solutions with telecoms and IT services provider DETASAD (Detecon Al Saudia Co. Ltd.) (https://www.detasad.com/) in Saudi Arabia. This was augmented by a launch in Saudi Arabia announced on 2nd November 2023.

Arqit participation in cross-border quantum-safe digital data transfer

15 June 2023: Arqit provided the symmetric key 'seal' in a pilot transfer of electronic trade documents - an electronic bill of lading (eBL) and a digital promissory note – between the UK and Singapore, reconciled using a Distributed Ledger (DLT) and paper verification. The trial was coordinated between the UK International Chamber of Commerce, Centre for Digital Trade and Innovation (C4DTI, and Singapore Government Infocomm Media Development Authority (IMDA).

AIEE Arqit QuantumCloud™ licence

15 June 2023: Kuwait-based Advanced International Electronic Equipment Company WLL (AIEE), (https://www.aiee.com) licences Arqit's QuantumCloud™ Symmetric Key Agreement Platform.

SNC MS strategic agreement

30 August 2023: strategic collaboration with Sierra Nevada Corporation Mission Systems UK, LTD. (SNC MS UK, https://www.sncmsuk.com/) to develop security solutions and services.

SecureCloud+ strategic agreement

6 September 2023: partnership and supply contract with SecureCloud+ (https://securecloudplus.co.uk/) a UK-based provider of secure defence collaboration services.

Exclusive Networks North America distribution agreement

11 September 2023: distribution agreement with Exclusive Networks N. America (EXN.PA, (https://www.exclusive-networks.com/usa/) for Arqit Symmetric Key Agreement Platform. Exclusive Networks is a €1.7bn market cap specialist in cyber security with €4.5bn in FY22 revenue and operations in Europe (€3.5bn FY22 revenue), the Americas (€0.53bn) and Asia-Pacific (€0.48bn).

Babcock International defence software integration with Arqit SKAP

7 December 2023: Arqit reports that Babcock demonstrated its *SwarmCore* network software – a project was created in collaboration with Arqit supported by Innovate UK - at the UK MOD BattleLab site. SwarmCore is used to control single or entire fleets of vehicles such as drones. Integration with Arqit's Symmetric Key Agreement Platform means that were a single vehicle either hacked or attacked the rest of the fleet would not be compromised.

BT, Fortinent launch quantum-safe VPN

14 December 2023: Collaboration with Arqit to launch a commercially available quantum-safe VPN. The collaboration brings to BT Fortinet's *FortiGate Next-Generation Firewalls* technology, backed by Arqit Network Secure™ to offer end-to-end VPN encryption security. This follows the successful conclusion of trials between BT's sites in London, Exeter, and Ipswich (Adastral Park).

Phalanx reseller agreement

10 January 2024: reseller agreement with Phalanx Solutions (https://getphalanxsolutions.com/) for Arqit's Symmetric Key Agreement Platform and NetworkSecure™ Adaptor.

Ampliphae 5G network security project

23 January 2024: completion of the *Security Enhanced Virtualised Networking for 5G* (SEViN-5G) project for quantum-safe security for Private 5G networks with network cyber security solutions provider Ampliphae Ltd., to provides a high-speed, scalable and secure platform for IoT applications and enterprise solutions.

Carahsoft agreement for US public sector

5 February 2024: agreement with Trusted Government IT Solutions Provider® Carahsoft Technology Corp., (https://www.carahsoft.com) today announced an agreement in which Carahsoft will be Arqit's Master Government Aggregator® making Arqit's Symmetric Key Agreement Platform available through Carahsoft's reseller partners and NASA Solutions for Enterprise-Wide Procurement (SEWP) V, Information Technology Enterprise Solutions – Software 2 (ITES-SW2), National Association of State Procurement Officials (NASPO) ValuePoint, E&I Cooperative Services Contract and OMNIA Partners contracts.

Mobile World Congress GLOMO Awards

28 February 2024: at the major 2024 annual MWC conference Arqit won Global Mobile Awards ('Glomo's) for both *Best Mobile Security Award* (ahead of Hiya, Nokia, SK Telecom, SAPEON and Vox Solutions) and 'top prize' of the year, the *CTO Choice Award*, selected from the winners of all seven categories of mobile Glomo.

This established Arqit's credentials at the most public and prestigious event in the mobile communications calendar (https://www.mwcbarcelona.com/mobile-awards):

2024 Mobile World Congress Arqit awards

Source: https://www.mwcbarcelona.com/mobile-awards.

Arqit's hypothetical valuation

We address the question of an appropriate valuation based on a combination of:

- The projected value of the cybersecurity market in 2025, at US$228bn (source: Arqit Quantum Inc., Form 20-F No. 001-40777 pp29, Gartner Group estimates).
- A hypothetical Arqit future revenue benchmark of c.US$100m, with an implied EBITDA of US$36.5m (based on industry peer group data). *This revenue benchmark is not time specific*.
- The market cap-weighted average EV/Revenue of 18 quoted representative cybersecurity providers, based on +1 year forecasts (*source: Koyfin*) currently 13.0x.

Using this methodology indicates an Equity Development hypothetical 'Fair Value' of:

- US$1.296bn or US$9.18 per share based on 131.5m year end FY23 weighted average (non-diluted) shares in issue[2].
- Indicative of an EV/Revenue multiple of 13.0x and median EV/EBITDA multiple of 35.4x.

Peer group comparative valuations

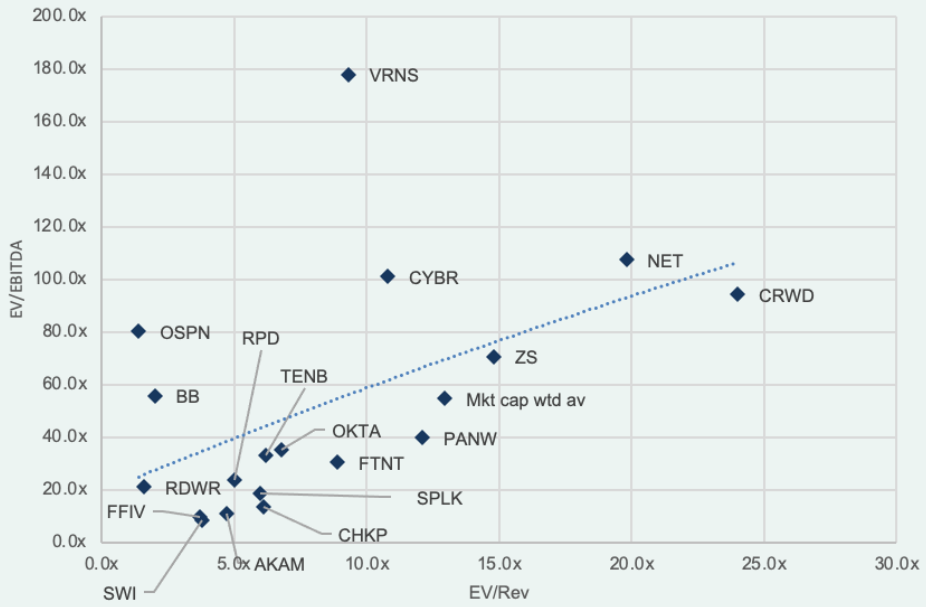
Ticker	Company	Price (£/$)	Mkt cap (£m)	EV/Rev	EV/EBITDA	PE
PANW	Palo Alto Networks Inc.	304.00	77,409	12.1x	40.1x	54.6x
CRWD	CrowdStrike Holdings Inc.	314.55	59,605	24.0x	94.6x	89.1x
ZS	Zscaler Inc.	219.07	25,641	14.8x	70.8x	78.9x
NET	Cloudflare Inc.	97.83	26,066	19.8x	107.5x	167.9x
OKTA	Okta Inc.	109.25	14,254	6.8x	35.4x	47.5x
SPLK	Splunk Inc.	156.11	20,760	6.0x	18.6x	25.0x
AKAM	Akamai Technologies Inc.	111.14	13,228	4.7x	10.9x	16.5x
CHKP	Check Point Software Tech.	158.91	14,670	6.1x	13.7x	17.5x
FFIV	F5 Inc.	187.08	8,681	3.7x	10.0x	14.8x
CYBR	CyberArk Software Ltd.	262.44	8,496	10.8x	101.3x	149.6x
RPD	Rapid7 Inc.	46.46	2,880	5.0x	23.9x	27.2x
TENB	Tenable Holdings Inc.	38.00	4,452	6.2x	33.1x	44.7x
BB	BlackBerry Limited	2.18	1,294	2.0x	55.9x	0.0x
SWI	SolarWinds Corporation	9.45	1,574	3.8x	8.4x	12.4x
VRNS	Varonis Systems Inc.	39.47	4,306	9.3x	178.1x	397.9x
RDWR	Radware Ltd.	13.97	587	1.6x	21.1x	27.2x
OSPN	OneSpan Inc.	7.61	303	1.4x	80.3x	15.2x
FTNT	Fortinet Inc.	54.45	41,544	8.9x	30.5x	40.4x
	Mkt cap wtd average			**13.0x**	**55.0x**	**69.7x**

Source: Koyfin 01-03-2024.

[2] **Summary calculation:**

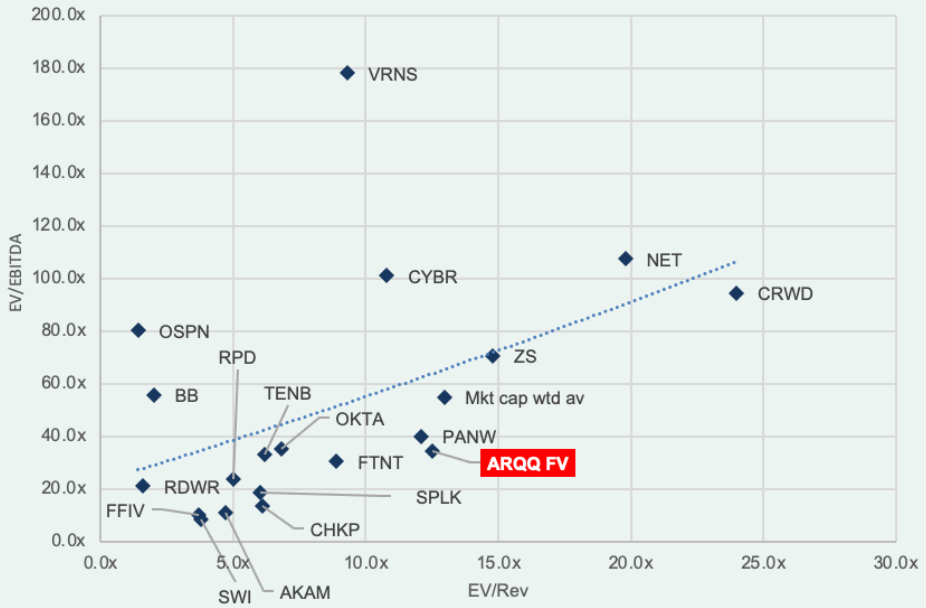
- Estimated 2025-26 US cybersecurity market value of US$262bn.
- Arqit Quantum Inc., hypothetical future revenue benchmark of US$100m, an implied market share, of 0.038%.
- Revenue multiple, market cap-weighted sample of 18 companies: 13.0x.
- Per share value based on reported FY23 year-end weighted average shares in issue.

Peers relative valuation, EV/EBITDA, EV/Revenue, +1 year prospective



Source: Koyfin

Peers relative valuation, including ARQQ at ED hypothetical Fair Value



Source: Koyfin, Equity Development estimates.

Financial summary

P&L

Yr to 30 Sep, US$m	2020	2021	2022	2023
Revenue	0.000	0.000	7.212	0.640
Other operating income	1.964	0.000	0.000	0.053
Revenue	**1.964**	**0.048**	**7.212**	**0.693**
Gross Sum	1.964	0.048	7.212	0.693
Operating costs				
Staff	(3.090)	(10.936)	(21.148)	(24.187)
Legal & Professional	(0.424)	(4.733)	(6.355)	(12.415)
Forex	0.010	(0.623)	(13.535)	8.764
Property	(0.159)	(0.187)	(0.754)	(2.289)
Other	(0.517)	(1.340)	(11.071)	(10.278)
Capitalised within intangibles	1.534	3.478	4.920	1.956
Share-based payments	(0.122)	(0.165)	(21.742)	(14.118)
Depreciation	(0.005)	(0.053)	(0.369)	(0.901)
Dep & Amortisation RoU	0.000	0.000	(0.923)	(1.733)
Sum Operating Costs	**(2.773)**	**(14.559)**	**(70.977)**	**(55.201)**
Reverse acquisition expense	0.000	(155.460)	0.000	0.000
Listing	0.000	(2.590)	0.000	0.000
EBIT Reported	(0.809)	(172.561)	(63.765)	(84.444)
EBIT Adjusted	**(0.687)**	**(172.396)**	**(42.023)**	**(70.326)**
Depreciation	(0.005)	(0.053)	(0.369)	(0.369)
Dep & Amortisation RoU	0.000	0.000	(0.923)	(0.923)
EBITDA Reported	(0.804)	(172.508)	(62.473)	(83.152)
EBITDA Adjusted	**(0.682)**	**(172.343)**	**(40.731)**	**(69.034)**
Financial income	0.065	0.000	0.000	0.041
Financial expense	(0.393)	(1.078)	(0.221)	(0.284)
One-off (warrant fair value)	0.000	(98.090)	117.394	10.638
PBT Reported	(1.137)	(271.729)	53.408	(74.049)
PBT Adjusted	**(1.015)**	**(173.474)**	**75.150**	**(59.931)**
Tax (adj)	0.569	0.000	0.000	0.141
Tax	0.569	0.000	0.000	0.141
Reported tax rate	0.000	0.000	0.000	0.000
Tax rate % adjusted	0.000	0.000	0.000	0.000
Forex	0.053	0.385	3.101	(1.567)
PAT Reported	(0.515)	(271.344)	68.176	(71.960)
PAT Adjusted	**(0.393)**	**(173.089)**	**89.918**	**(57.842)**
Basic wtd. av. shares (m)	59.2608	68.3264	121.1613	131.4689
Dilutive (m)	0.0000	0.0000	13.0389	13.0389
Diluted wtd. av. shares (m)	59.2608	68.3264	134.2002	144.5078
EPS rptd. basic ($c)	**(0.96)**	**(397.69)**	**53.71**	**(56.22)**
EPS rptd. diluted ($c)	(0.96)	(397.69)	48.49	(51.14)
EPS adj. basic ($c)	(0.75)	(253.89)	71.65	(42.80)
EPS adj. diluted ($c)	(0.75)	(253.89)	64.69	(38.94)

Source: Company data. Form 20F.

Cashflow

Yr to 30 Sep, US$m	2020	2021	2022	2023
PBT	(1.137)	(271.729)	53.408	(74.049)
One-off (warrant fair value)	0.000	98.090	(117.394)	(10.638)
Share option charge	0.122	0.165	21.742	14.118
Depreciation	0.005	0.053	1.292	2.634
Finance income	(0.065)	0.000	0.000	(0.041)
Interest	0.393	1.078	0.221	0.284
Other	0.000	155.460	11.667	33.398
Operating Cash Flow	**(0.682)**	**(16.883)**	**(29.064)**	**(34.294)**
Working capital				
(Increase)/Decrease in receivables	(0.173)	(6.132)	(17.949)	21.136
Increase/(Decrease) in payables	(1.285)	(1.290)	5.586	(7.982)
Movement in working capital	**(1.458)**	**(7.422)**	**(12.363)**	**13.154**
Cash from operations	**(2.140)**	**(24.304)**	**(41.427)**	**(21.140)**
Forex	(0.028)	0.269	14.708	(11.685)
Tax (paid)/received	0.833	0.000	0.000	0.000
Net cash from operations	(1.334)	(24.035)	(26.719)	(32.784)
Investing activities	0.000	0.000	0.000	0.000
PPE	(0.026)	(0.223)	(2.376)	(0.712)
Intangibles	(4.544)	(9.082)	(22.056)	(15.411)
Net cash used in investing	**(4.571)**	**(9.305)**	**(24.432)**	**(16.123)**
Net OpFCF	(5.905)	(33.340)	(51.151)	(48.907)
Financing activities				
Shares	0.000	0.000	21.306	45.080
Convertible loans	0.646	14.148	0.000	0.000
Borrowing/Leases	1.034	5.042	(0.657)	(1.599)
Borrowing repaid	0.000	(6.120)	0.000	0.000
Funds acquired/other	0.000	107.035	1.527	1.372
Net cash from financing	1.680	120.105	22.176	44.853
Forex	0.193	0.006	(9.025)	(0.457)
Net increase in cash	(4.032)	86.771	(38.000)	(4.511)
Cash at beginning of year	4.227	0.195	86.966	48.966
Cash at year end	**0.195**	**86.966**	**48.966**	**44.455**

Source: Company data. Form 20F.

Balance sheet

Yr to 30 Sep US$m	2020	2021	2022	2023
Fixed Assets				
Intangibles gross	8.777	18.235	40.291	3.503
Amortisation	0.000	0.000	0.000	0.000
Intangible assets	8.777	18.235	40.291	3.414
PPE gross	0.032	0.256	2.591	3.260
Depreciation	(0.005)	(0.057)	(0.385)	(1.296)
PPE net	0.027	0.199	2.206	1.964
Investments	0.032	0.034	0.028	0.030
Other	0.000	5.000	24.704	8.028
Sum Fixed Assets	**8.836**	**23.468**	**67.229**	**13.436**
Current Assets				
Trade receivables	0.280	3.292	7.677	3.217
Assets for sale	0.000	0.000	0.000	38.677
Cash, Equivalents	0.195	86.966	48.966	44.455
Sum Current Assets	**0.475**	**90.258**	**56.643**	**86.349**
Total Assets	9.311	113.726	123.872	99.785
Current Liabilities				
Trade payables	(2.386)	(17.069)	(22.655)	(18.831)
Borrowings/Leases	(5.460)	0.000	(1.154)	(7.987)
Tax, Other	0.000	0.000	0.000	0.000
Sum Current Liabilities	**(7.846)**	**(17.069)**	**(23.809)**	**(26.818)**
Total Assets less Current Liabilities	1.466	96.657	100.063	72.967
Long-term Liabilities				
Borrowings / Leases	0.000	0.000	0.000	0.000
Warrants	0.000	(128.038)	(10.644)	(0.024)
Payables	(0.534)	(2.460)	(4.183)	(0.006)
Leases	0.000	0.000	(6.681)	(6.284)
Sum Long-term liabilities	**(0.534)**	**(130.498)**	**(21.508)**	**(6.314)**
Total liabilities	(8.380)	(147.567)	(45.317)	(33.132)
Net Assets	0.931	(33.841)	78.555	66.653
Capital & Reserves				
Share Capital	0.000	0.011	0.012	0.016
Convertible loans, other	1.411	0.000	0.000	0.000
Currency / other reserves	(0.129)	167.061	170.161	168.594
Share Premium	0.000	70.999	92.306	137.021
Share option reserve	0.135	0.303	23.216	38.555
Retained earnings	(0.486)	(272.215)	(207.140)	(277.533)
Equity	**0.930**	**(33.840)**	**78.555**	**66.653**

Source: Company data. Form 20F.

Appendix I: RFC 8784

Discussion of RFC 8784; extract from PaloAlto Tech Docs.

"The essence of RFC 8784 is exchanging static post-quantum pre-shared keys (PQ PPKs) out of band, separately from the IKE key exchange, and mixing the out of band PQ PPK material with the classical Diffie-Hellman (DH) key material that is transmitted in band during the IKEv2 key exchange. This enhances the key exchange in two ways:

- A DH key and variants of DH keys rely on the difficulty of solving the discrete log problem, such as solving for the very large prime numbers on which DH is based. However, with the advent of cryptographically relevant quantum computers (CRQCs), DH keys become vulnerable to attacks based on Shor's algorithm. Implementing RFC 8784 enhances the cryptographic strength of the key because the mixed key is no longer based solely on the difficulty of solving the discrete log problem (e.g., solving for very large prime numbers), so the mixed key isn't vulnerable to Shor's algorithm.

- A listener, or man-in-the-middle, can't harvest all of the key material to decrypt later. The classical DH portion of the key is sent in the IKE peering key exchange, but the PQ PPK that the IKE peers mix with the DH key material is never transmitted during the key exchange or in the VPN after it's been established, so even with the DH portion of the key material, attackers can't decrypt the data that traverses the VPN.

The IKEv2 peers know which PQ PPK to use based on a Key ID. Each PQ PPK consists of two elements, a KeyID and a pre-shared secret. The pre-shared secret is the key material that you share with the IKEv2 peer out of band. It is never transmitted in band with the DH key material or with the data after establishing the VPN. Instead, the administrator of one IKEv2 peer manually creates the static pre-shared secret and communicates it securely, for example by secure email or by pushing from Panorama to the administrator of the other IKEv2 peer. Each administrator programs the pre-shared secret into their peer, so the secret is never revealed in the IKE connection.

The Key ID, which is transmitted in band during the key exchange, identifies the pre-shared secret on the IKEv2 peer. The IKEv2 peer uses the Key ID to look up the pre-shared secret and mixes it with the DH key material to create new key material that isn't based on prime numbers and can't be stolen by eavesdropping on the communication.

This standards-based method provides an easy way to prevent attackers from eavesdropping on the connection and intercepting the keys, which would allow attackers to decrypt the data sent in the VPN after it's established, while also ensuring interoperability with other devices that adhere to the standard."

Source https://docs.paloaltonetworks.com/network-security/quantum-security/administration/quantum-security-concepts/how-rfc-8784-resists-quantum-computing-threats

Contacts

Andy Edmond
Direct: 020 7065 2691
Tel: 020 7065 2690
andy@equitydevelopment.co.uk

Hannah Crowe
Direct: 0207 065 2692
Tel: 0207 065 2690
hannah@equitydevelopment.co.uk

Equity Development Limited is regulated by the Financial Conduct Authority

Disclaimer

Equity Development Limited ('ED') is retained to act as financial adviser for its corporate clients, some or all of whom may now or in the future have an interest in the contents of this document. ED produces and distributes research for these corporate clients to persons who are not clients of ED. In the preparation of this report ED has taken professional efforts to ensure that the facts stated herein are clear, fair and not misleading, but makes no guarantee as to the accuracy or completeness of the information or opinions contained herein.

This document has not been approved for the purposes of Section 21(2) of the Financial Services & Markets Act 2000 of the United Kingdom ('FSMA'). Any reader of this research should not act or rely on this document or any of its contents. This report is being provided by ED to provide background information about the subject of the research to relevant persons, as defined by the Financial Services and Markets Act 2000 (Financial Promotions) Order 2005. This document does not constitute, nor form part of, and should not be construed as, any offer for sale or purchase of (or solicitation of, or invitation to make any offer to buy or sell) any Securities (which may rise and fall in value). Nor shall it, or any part of it, form the basis of, or be relied on in connection with, any contract or commitment whatsoever.

Research produced and distributed by ED on its client companies is normally commissioned and paid for by those companies themselves ('issuer financed research') and as such is not deemed to be independent as defined by the FCA but is 'objective' in that the authors are stating their own opinions. This document is prepared for clients under UK law. In the UK, companies quoted on AIM are subject to lighter due diligence than shares quoted on the main market and are therefore more likely to carry a higher degree of risk than main market companies.

ED may in the future provide, or may have in the past provided, investment banking services to the subject of this report. ED, its Directors or persons connected may at some time in the future have, or have had in the past, a material investment in the Company. ED, its affiliates, officers, directors and employees, will not be liable for any loss or damage arising from any use of this document to the maximum extent that the law permits.

More information is available on our website www.equitydevelopment.co.uk

Equity Development, 2nd Floor, Park House, 16-18 Finsbury Circus, London, EC2M 7EB

Contact: info@equitydevelopment.co.uk | 0044 207 065 2690