

Stocktake on European Randomness Expectations

Non-technical reading for Boards/CxOs

Santosh Pandit, Founder, BeatQuantum. 17 September 2026.

Every encryption key, every digital signature and every secure connection starts with a random number. If the random number can be guessed, the key can be guessed, and all the investment on top is ineffective. And that would impact you as a senior CxO or Board level stakeholders.

Most organisations spend time on algorithms, key lengths and the quantum transition. Very little of that time reaches the question of where the randomness comes from and how anyone knows it is good enough.

This stocktake sets out what European authorities expect, what European and UK regulations and guidance say, and what that means for you as a decision maker who is being offered "certified" or "quantum" randomness products. **The short answer is that Europe cares about the quality of the output and, with one exception, does not tell you where the randomness has to come from.**

What randomness is, in one paragraph

A computer cannot invent unpredictability. It has to collect it from somewhere physical: electronic noise, timing jitter inside the processor, a dedicated chip, or, in the newest products, a quantum optical effect. **Anything that is random not only once but also on an ongoing basis. That raw collection is called the entropy source.** It is then fed into a deterministic algorithm that stretches it into as many random numbers as the system needs. Every serious authority treats these as two separate things: the source, whose quality is hard to prove, and the algorithm on top, whose quality is relatively easy to prove. Almost all of the regulatory attention sits on the second. At BeatQuantum we take both seriously.

What the law says

The horizontal European and UK laws do not mention randomness at all. This is why your teams are unlikely to focus on randomness without expert guidance.

- **DORA** requires financial entities to have an encryption policy and a key management policy that covers generating keys, among nine other lifecycle steps. It sets no quality standard for the generation step.
- **The Cyber Resilience Act** requires products to use "state of the art" encryption. The only reference to random number generation in the whole CRA framework is in a November 2025 implementing regulation, where it appears as an example of a security function that a microprocessor, microcontroller or similar chip might have.
- **NIS2** requires policies on the use of cryptography and, for the digital infrastructure sectors, a key management method for "generating different keys". Nothing on how.
- **The UK Cyber Security and Resilience Bill**, now in the House of Lords, contains no cryptography wording of any kind. The detail is left to future regulations and a code of practice that have not been drafted.
- **eIDAS** comes closest, and only by implication: signature creation data for qualified signatures must be such that it "can practically occur only once".

Randomness requirements live one level down, in certification schemes and in the technical guidance of national authorities. That is where the differences between countries appear.

Summary table by country

COUNTRY	AUTHORITY	POSITION ON RANDOMNESS	PRESCRIBES THE SOURCE?	ROUTE TO DEMONSTRATE QUALITY
Austria	Federal Chancellery (Information Security Handbook)	Key generators must produce statistically uniform output over the whole key space; a noise source with post-processing and testing is given as the example.	No	None named
Belgium	Centre for Cybersecurity Belgium	No published position on randomness; the 2025 quantum white paper it contributed to is silent on it.	No	None named
European Union (cross-border)	SOG-IS and the ECCG under ENISA (Agreed Cryptographic Mechanisms)	A physical source should only be used to seed and reseed an approved algorithm; direct use of raw output is "not agreed". Minimum seed strength is set (125 bits; 188 bits where quantum resistance is required).	No, only what is done with it	Common Criteria evaluation under the EUCC scheme

COUNTRY	AUTHORITY	POSITION ON RANDOMNESS	PRESCRIBES THE SOURCE?	ROUTE TO DEMONSTRATE QUALITY
France	ANSSI	The March 2026 rules make a post-processing algorithm with a protected internal state mandatory and exclude the use of an unprocessed physical generator. The physical source must be documented and tested; a reasoned justification of its quality is recommended. A source evaluated under the German method is presumed compliant.	No, but the processing architecture is mandatory	Common Criteria under the French scheme, which uses the German evaluation method
Germany (the exception)	BSI	The only full framework in Europe. Physical, non-physical and deterministic generators are divided into named quality classes, each with a required mathematical model, live health tests and minimum entropy figures. The classes are binding in German certification and adopted by France, the Netherlands and Spain. The January 2026 guideline no longer recommends the lower of the two physical classes for general use.	Yes, by class: the source must be evaluated against a named class with its model and tests; no particular physical process is named	Common Criteria certification against the BSI classes
Italy	ACN	No published position on randomness in its cryptographic or post-quantum guidance.	No	None named
Netherlands	NCSC-NL and AIVD	Randomness is addressed inside the TLS guidelines: identify the generator your software uses, confirm it is unpredictable, and use a hardware generator where load is high. Central government cryptography policies must address random number generation, with no technical detail.	No	Common Criteria under the Dutch scheme, which uses the German classes
Norway	NSM	Collect bits from a physical process with enough unpredictability and feed a well-studied generator; use dedicated hardware where available, otherwise the operating system generator; estimating entropy is described as difficult.	No	Refers to the US NIST standards
Spain	CCN	The authorised mechanisms guide is reported to adopt the German quality classes; the CCN product catalogue lists qualified randomness hardware. The guide itself sits behind an access gate and could not be read for this stocktake.	Reported yes, unverified	National product qualification (CPSTIC)
Sweden	MCF and the Armed Forces	No public position; defence requirements are unpublished.	No	None named
Switzerland	BACS	Quantum random number generators are "explicitly not" a solution to the quantum computing threat, while having niche uses. No general randomness guidance.	No	None named

COUNTRY	AUTHORITY	POSITION ON RANDOMNESS	PRESCRIBES THE SOURCE?	ROUTE TO DEMONSTRATE QUALITY
United Kingdom	NCSC	Classical random number generators "continue to meet our needs" for government and military use, stated in 2020 and restated in 2025. The 2020 paper states that quantum generators offer no new mitigation against quantum computers; the 2025 paper adds that they may offer higher rates and faster detection of source degradation, and that research should continue. Device makers should use a trusted entropy source such as one meeting the US NIST recommendations; pre-shared keys need at least 128 bits of entropy. The one UK scheme that audited entropy sources, for smart meters, has passed out of NCSC's hands.	No	Refers to the US NIST standards; no live UK scheme

Positions as published by each authority; verified 17 September 2026.

Three patterns in the table

Germany prescribes how the source must be evaluated; everyone else describes the outcome. BSI names the quality classes a generator must meet and the evidence a vendor must supply, without naming a physical process. France comes next, with a mandatory architecture but no rule on the source. The rest of Europe, including the UK, states the outcome required and points to someone else's standard, most often the American NIST series, for the detail.

Nobody in Europe requires a quantum source, and the three authorities that have commented on quantum sources are sceptical. The UK says classical generators are sufficient, while welcoming further research on quantum sources. Switzerland says quantum generators are not a quantum-threat mitigation. BSI's own page on the subject says that the claim "based on the laws of nature, therefore secure" is wrong, and its 2024 classification refuses to distinguish quantum entropy from any other physical entropy. France certified a quantum chip in February 2026, as an ordinary physical generator, and the certificate report states that certification is not a recommendation.

The entropy certificate that vendors most often hold is American. The NIST Entropy Source Validation register (known as the **ESV register**) is the document most randomness vendors point to, because a FIPS 140-3 module cannot be certified without one. European certificates exist, through Common Criteria against the German classes and through the Spanish product catalogue, and fewer vendors hold them. The American register has no legal standing in

Europe, and it admits software timing sources as readily as hardware chips. Several UK quantum randomness vendors have no entry on it at all.

What this means for a decision maker

With the exception of Germany, European countries are non-prescriptive about the sources of randomness. The European preference is for the quality of the outcome rather than the source. A product that seeds a well-studied algorithm from a documented, tested source meets the guidance of every authority in the table; where certification is required, Germany and France also ask for a defined evidence package for the source. A product that sells the source alone, however exotic, satisfies none of them on its own.

And in my view this is a great news for European Boards and CxOs. You are not being forced to invest in a particular technology and retain that option where your business cases justifies its use.

The American validation register has no binding applicability in Europe, and a certificate on it says nothing about how the product behaves once installed in your environment. The practical course is to evaluate your entropy from a statistical perspective, in your own deployment, and to establish good practice in how it is deployed: seed a recognised algorithm, keep the source documented, watch for the failure modes the authorities have written up (virtual machines starved of entropy, keys generated before the system has finished starting, processor generators that silently return zeros), and treat certifications as one input rather than as the answer. The German classes and the American register tell you a design was sound on the day it was tested. Your own measurement tells you it is sound today.

The BeatQuantum approach

As the world-leading Centre of Excellence in Applied Post-Quantum Cryptography, we have implemented almost every algorithm accepted by every authority in Europe, and by the other international jurisdictions we track. The natural question is what BeatQuantum does about its own randomness.

Our research and experimentation on randomness began many years ago. Since 2025, kyber.club has offered free cryptographic key pairs for the FIPS 203, FIPS 204 and FIPS 205 algorithms and for FrodoKEM; we have found no earlier public service doing so. The output of the generator behind those keys was tested on 9 March 2025 against the NIST Statistical Test Suite (SP 800-22) on a 100 MB sample of 838 streams and passes all 15 tests; the full results are published on the site. A statistical suite checks the output for detectable defects and does

not measure the entropy of the source. **We treat that result as a check on the quality of the outcome, repeated in our own deployment, and not as a certificate.** We also offer free random numbers at kyber.club/random to anyone who wants to use them or run their own tests.

We share the view of NCSC UK, and of most of the authorities in the table, that **cryptographically secure pseudo-random number generators are sufficient for all practical purposes now and in the post-quantum era.** We also share the researchers' DNA, so we remain open to adding further sources of entropy, hardware-based or otherwise, on one condition: the measured quality of the overall outcome must improve rather than deteriorate. A new source earns its place by the same test we apply to the existing one.

So whether you are a free user at kyber.club or an enterprise customer of beatquantum.com, our advice and our services on randomness exceed the regulatory minimum set out in this stocktake.

Sources

National authorities

- NCSC UK, Quantum security technologies, white paper, March 2020.
<https://www.ncsc.gov.uk/paper/quantum-security-technologies>
- NCSC UK, Quantum networking technologies, white paper, August 2025 (updated April 2026).
<https://www.ncsc.gov.uk/paper/quantum-networking-technologies>
- NCSC UK, Device security principles for manufacturers, protect data at rest and in transit, v2.1, February 2025.
<https://www.ncsc.gov.uk/collection/device-security-principles-for-manufacturers/protect-data-at-rest-and-in-transit>
- NCSC UK, Using IPsec to protect data, December 2025.
<https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data>
- BSI, A Proposal for Functionality Classes for Random Number Generators, Version 3.0, September 2024.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e_2024.pdf
- BSI, TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2026-01, January 2026.
<https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf>
- BSI, Quantenzufallszahlengeneratoren (position page on quantum random number generators).
<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten->

Kryptografie/Quantenkryptografie/Quantenzufallszahlengeneratoren/quantenzufallszahlengeneratoren_node.html

- ANSSI, ANSSI-PG-083 Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 3.00, March 2026.
<https://messervices.cyber.gouv.fr/documents-guides/anssi-guide-mecanismes-crypto-3.00.pdf>
- ANSSI, Rapport de certification ANSSI-CC-2026/01 (IDQ20MC1), February 2026.
<https://messervices.cyber.gouv.fr/visas/ANSSI-CC-2026-01-rapport.pdf>
- NCSC-NL, IT Security Guidelines for Transport Layer Security, version 2025-05.
https://www.ncsc.nl/api/media/sites/default/files/Publication_TLS-Security%20guidelines-2025-05_ENG.pdf
- Ministry of the Interior and Kingdom Relations (Netherlands), Rijksbreed Beleidskader Cryptografie, March 2025.
<https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2025/03/Rijksbreed-Beleidskader-Cryptografie.pdf>
- SOG-IS, Agreed Cryptographic Mechanisms, v1.3, February 2023.
<https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf>
- ECCG (ENISA), Agreed Cryptographic Mechanisms, version 2.0, April 2025.
https://certification.enisa.europa.eu/document/download/a845662b-ae0-484e-9191-890c4cfa7aaa_en?filename=ECCG+Agreed+Cryptographic+Mechanisms+version+2.pdf
- BACS (Switzerland), Quantum computers and post-quantum cryptography, technology brief, December 2025.
<https://www.bacs.admin.ch/dam/en/sd-web/hVD1MMR21Uab/technologiebetrachtung-qcpgc-en.pdf>
- NSM (Norway), NSM Cryptographic Recommendations, v2.0, March 2025.
<https://nsm.no/getfile.php/1314334-1742808614/NSM/Filer/Dokumenter/Veiledere/NSM%20Cryptographic%20Recommendations%202025.pdf>
- Federal Chancellery (Austria), Österreichisches Informationssicherheitshandbuch, v4.4.0, November 2023.
<https://www.sicherheitshandbuch.gv.at/>

Legislation

- Regulation (EU) 2022/2554 (DORA).
<https://eur-lex.europa.eu/eli/reg/2022/2554/oj>
- Commission Delegated Regulation (EU) 2024/1774 (DORA RTS on ICT risk management).
https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj
- Regulation (EU) 2024/2847 (Cyber Resilience Act).
<https://eur-lex.europa.eu/eli/reg/2024/2847/oj>
- Commission Implementing Regulation (EU) 2025/2392 (CRA technical descriptions of product categories).
https://eur-lex.europa.eu/eli/reg_impl/2025/2392/oj
- Directive (EU) 2022/2555 (NIS2).
<https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

- Commission Implementing Regulation (EU) 2024/2690 (NIS2 technical and methodological requirements).
https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj
- Regulation (EU) 2024/1183 (eIDAS 2).
<https://eur-lex.europa.eu/eli/reg/2024/1183/oj>
- Cyber Security and Resilience (Network and Information Systems) Bill, HL Bill 49.
<https://bills.parliament.uk/bills/4035>

Registers

- NIST Entropy Source Validation register.
<https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/search>
- Kyber Club, NIST SP 800-22 test results, March 2025.
<https://kyber.club/nist-test-results.pdf>