The MOSAIC Protocol: Building, Costing and Integrating a Multijurisdictional Cyber-Attribution Service

Supplementary Paper 3B

Christopher I. V. Farmer

Publication edition, August 2026

Contents

Abstract....4
Table of Authorities....5
Cases....5
Legislation....5
Treaties and International Instruments....6
Standards, Government and Technical Materials....6
1. From Doctrine to an Operating Service....10
1.1 Design Principles....11
1.2 What MOSAIC Does Not Claim....11
1.3 Operational Assumptions and Acceptance Tests....12
2. The System to Be Built....13
2.1 Custodian Gateway....14
2.2 National Node....15
2.3 Federation Layer....16
2.4 Decision Plane....17
2.5 Oversight Plane....17
2.6 Trust Registry, Message Integrity and Time....17
3. The Common Evidential Model....19
3.1 Source Classes....20
3.2 Confidence and Contrary Hypotheses....20
3.3 The Attribution Manifest....20
3.4 Chain of Custody....21
3.5 Correction, Challenge and Contamination....21
3.6 Evidential Graph, Provenance and Admissibility....22
4. Operating Workflows....23
4.1 Incident Intake....23
4.2 Federated Discovery....24
4.3 Emergency Preservation....25
4.4 Production and Legal Process....25
4.5 Public Attribution and Response Package....26
4.6 Manifest Deposit, Amendment and Opening....26
4.7 Correction Workflow....27
5. Security, Privacy and Abuse....27
5.1 Zero-trust Identity and Access....28
5.2 Encryption and Key Management....28
5.3 Secure Development and Supply Chain....28
5.4 Logging and Protective Monitoring....29
5.5 Privacy Engineering....29
5.6 Insider and Partner Abuse....30
5.7 Resilience and Disaster Recovery....30
5.8 Threat-led Assurance and Hostile-node Tests....30
6. Legal and Institutional Integration in the United Kingdom....32
6.1 Statutory Functions....32
6.2 Preservation Power....33
6.3 Incident Reporting and Secrecy....33
6.4 Controller and PMSC Duties....33
6.5 Courts, Disclosure and Evidential Weight....34
6.6 International Agreements....34

6.7 Rights, Retention and Constitutional Control....34
7. Costed Options....36
7.1 Twelve-month Pilot....36
7.2 Core Three-year Programme....37
7.3 Constrained and Extended Options....38
7.4 Benefits and the Cost of Absence....40
7.5 Procurement and Commercial Structure....40
7.6 Cost Method, Sensitivity and Affordability Gates....41
8. Delivery and Integration....42
8.1 Gate One: Foundation, Months 0–3....42
8.2 Gate Two: Alpha and Closed Exercise, Months 3–6....43
8.3 Gate Three: Beta Pilot, Months 6–12....43
8.4 Gate Four: Core Scale, Months 12–36....43
8.5 Integration Rather than Replacement....44
8.6 Legacy, Cloud and Operational-technology Integration....44
9. Testing, Evaluation and Public Measures....45
10. Failure Conditions and Objections....46
11. Conclusion....47
Bibliography....48
Books, Chapters and Articles....48

Abstract

Paper 3 argued that a hostile cyber operation may be divided amongst jurisdictions so that no territorial State possesses an intelligible view of it, whilst the controller, having designed the division, retains the only map capable of joining objective, target, code, infrastructure, payment and effect. The legal answer proposed there was a duty of correlation placed chiefly upon the actor which possesses that map, supported by authenticated notices, rapid preservation and federated enquiries between States. This paper supplies the machinery.

MOSAIC—the Multijurisdictional Operation Signal Attribution and Integrity Correlation protocol—is a federated public system through which authorised national nodes, designated providers and investigators can ask narrowly defined questions of evidence held elsewhere without first transferring the evidence itself. It is not a global database. Raw logs remain with the lawful custodian; the protocol exchanges signed enquiries, match assertions, provenance, confidence and preservation receipts. Production follows the legal process applicable to the requested evidence. The design thereby shortens the interval in which an ephemeral fragment disappears, without pretending that technical correlation proves legal attribution.

The paper specifies the service rather than merely recommending it. It defines the common event schema; the cryptographic operation identifier; the controller's attribution manifest; the national node; provider gateways; privacy-preserving matching; evidential chain of custody; human decision points; correction and challenge; zero-trust access; compromise recovery; independent oversight; and the interfaces by which the National Cyber Security Centre, National Crime Agency, courts, regulators, operators of essential services and foreign counterparts might employ it. STIX 2.1 and TAXII 2.1 provide an exchange foundation, but require legal-evidence and privacy extensions; existing MISP or OpenCTI deployments may serve as adapters, not as the final system of record.

A twelve-month United Kingdom-led pilot is estimated at £10.6 million including optimism-bias contingency. The core three-year programme—twelve national partners, approximately 2,000 reporting organisations, 250 million normalised security events each month and continuous operations—is estimated at £61.2 million in 2026 pounds, excluding VAT and the ordinary cost of participants' existing logs. A constrained deployment is estimated at £29.6 million; a thirty-State, high-volume deployment at £125.6 million. Each estimate discloses staffing, infrastructure, assurance, partner grants, contingency and the assumptions by which it may be challenged.

MOSAIC cannot make an unwilling State cooperate, determine intent from an address, or confer an international right to use force. It can do something more modest and, for immediate defence, more useful: preserve the fragment before it expires; reveal that apparently separate fragments form one campaign; show which actor possessed which knowledge at which time; and produce an auditable record by which sanctions, prosecution, civil restraint, diplomatic action and, where the independent rules of international law permit it, defensive force may be considered upon evidence rather than conjecture.

Keywords: cyber attribution; electronic evidence; federated systems; privacy-enhancing technology; operational technology; procurement; due diligence; State responsibility.

Table of Authorities

Cases

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) [2007] ICJ Rep 43, [430] 23

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Judgment) [2005] ICJ Rep 168 36

Big Brother Watch and others v United Kingdom (2022) 74 EHRR 17 35

Centrum för rättvisa v Sweden [GC] App no 35252/08 (25 May 2021) 35

Corfu Channel (United Kingdom v Albania) (Merits) [1949] ICJ Rep 4, 22 23

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; Kärntner Landesregierung (Joined Cases C-293/12 and C-594/12) EU:C:2014:238 35

La Quadrature du Net and others v Premier ministre and others (Joined Cases C-511/18, C-512/18 and C-520/18) EU:C:2020:791 35

Microsoft Corporation v United States 829 F 3d 197 (2d Cir 2016), vacated as moot 584 US 236 (2018) 35

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14 36

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others (Case C-623/17) EU:C:2020:790 35

Prokuratuur (Case C-746/18) EU:C:2021:152 35

R (KBR Inc) v Director of the Serious Fraud Office [2021] UKSC 2, [2022] AC 519, [21]–[27] 35

R v Shephard [1993] AC 380 (HL) 23

R v Spiby (1990) 91 Cr App R 186 (CA) 23

Roman Zakharov v Russia [GC] App no 47143/06 (4 December 2015) 35

SpaceNet AG and Telekom Deutschland GmbH (Joined Cases C-793/19 and C-794/19) EU:C:2022:702 35

Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson and others (Joined Cases C-203/15 and C-698/15) EU:C:2016:970 35

United States Diplomatic and Consular Staff in Tehran (United States of America v Iran) (Judgment) [1980] ICJ Rep 3, [68]–[74] 23

Legislation

Civil Evidence Act 1995 23

Clarifying Lawful Overseas Use of Data Act 2018, Pub L No 115-141, div V, 132 Stat 1213 12

Computer Misuse Act 1990 32

Crime (Overseas Production Orders) Act 2019 ..... 12, 35

Criminal Justice Act 2003 23

Criminal Procedure and Investigations Act 1996 23

Data Protection Act 2018 ..... 29, 35

Data (Use and Access) Act 2025 29

Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on designated establishments and legal representatives for gathering electronic evidence in criminal proceedings [2023] OJ L191/181 12

Freedom of Information Act 2000 35

Human Rights Act 1998 29

Investigatory Powers Act 2016, as amended by the Investigatory Powers (Amendment) Act 2024 32

National Security Act 2023 32

Official Secrets Act 1989 35

Procurement Act 2023 42

Public Records Act 1958 35

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191/118 12

UK GDPR arts 5 and 25, as amended by the Data (Use and Access) Act 2025 ..... 15, 22, 29

Treaties and International Instruments

Charter of the United Nations arts 2(4) and 51 36

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) art 8 29

Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004) ETS No 185 ..... 12, 34

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (opened for signature 12 May 2022) CETS No 224 12

Standards, Government and Technical Materials

Annabelle Backman and others, ‘HTTP Message Signatures’ (RFC 9421, February 2024)

Ben Laurie, Emilia Messeri and Rob Stradling, ‘Certificate Transparency Version 2.0’ (RFC 9162, December 2021)

Brian Campbell and others, ‘OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens’ (RFC 8705, February 2020)

Cabinet Office and Government Commercial Function, *The Sourcing Playbook* (updated 15 June 2026)

Cabinet Office, ‘The Technology Code of Practice’ https://www.gov.uk/guidance/the-technology-code-of-practice accessed 5 August 2026

Carlisle Adams and others, ‘Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)’ (RFC 3161, August 2001)

Cloud Security Alliance, *Cloud Controls Matrix v4.0.12* (2024)

Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime* (CETS No 224, 2022)

Council of Europe, *Guide to the Implementation of the Second Additional Protocol to the Convention on Cybercrime in Domestic Law* (2025)

Cybercrime Convention Committee, *24/7 Points of Contact Network of the Budapest Convention on Cybercrime: Assessment Report* (T-CY(2020)2, 2020)

Cybersecurity and Infrastructure Security Agency, *2026 Minimum Elements for a Software Bill of Materials* (July 2026)

Cybersecurity and Infrastructure Security Agency and others, *Adapting Zero Trust Principles to Operational Technology* (29 April 2026)

Cybersecurity and Infrastructure Security Agency and others, *Best Practices for Event Logging and Threat Detection* (21 August 2024)

Cybersecurity and Infrastructure Security Agency, *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software* (2023)

Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model Version 2.0* (April 2023)

Torsten Lodderstedt, John Bradley, Andrey Labunets and Daniel Fett, 'Best Current Practice for OAuth 2.0 Security' (RFC 9700, January 2025)

Department for Science, Innovation and Technology, 'Cyber Security and Resilience Bill' https://www.gov.uk/government/collections/cyber-security-and-resilience-bill accessed 5 August 2026

Department for Science, Innovation and Technology, 'Summary of the Cyber Security and Resilience Bill' (30 June 2026) https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill accessed 5 August 2026

Eric Rescorla, 'The Transport Layer Security (TLS) Protocol Version 1.3' (RFC 8446, August 2018)

European Union Agency for Cybersecurity, *Cooperative Models for Information Sharing and Analysis Centres* (ENISA 2018)

European Union Agency for Cybersecurity, *Pseudonymisation Techniques and Best Practices* (ENISA 2019)

Fang Liu and others, *NIST Cloud Computing Reference Architecture* (NIST SP 500-292, 2011)

Foreign, Commonwealth & Development Office, *Application of International Law to States' Conduct in Cyberspace: UK Statement* (3 June 2021)

Forum of Incident Response and Security Teams, *Traffic Light Protocol (TLP): FIRST Standards Definitions and Usage Guidance—Version 2.0* (2022)

Jim Schaad, 'CBOR Object Signing and Encryption (COSE): Structures and Process' (RFC 9052, August 2022)

Government Digital Service, *Artificial Intelligence Playbook for the UK Government* (10 February 2025)

Government Digital Service, 'Service Standard' https://www.gov.uk/service-manual/service-standard accessed 5 August 2026

Government Project Delivery, *Government Functional Standard GovS 002: Project Delivery* (version 2.1, 2025)

Government Project Delivery, *The Teal Book* (version 3.0, 2026)

Graham Klyne and Chris Newman, 'Date and Time on the Internet: Timestamps' (RFC 3339, July 2002)

HM Government, 'Secure by Design' https://www.security.gov.uk/policy-and-guidance/secure-by-design/ accessed 5 August 2026

HM Treasury, 'Green Book supplementary guidance: optimism bias' (21 April 2013) https://www.gov.uk/government/publications/green-book-supplementary-guidance-optimism-bias accessed 5 August 2026

HM Treasury, *The AQuA Book: Guidance on Producing Quality Analysis for Government* (2025)

HM Treasury, *The Green Book: Central Government Guidance on Appraisal and Evaluation* (2026) https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2026 accessed 5 August 2026

HM Treasury, *The Magenta Book: Central Government Guidance on Evaluation* (updated 15 May 2026)

HM Treasury, *The Orange Book: Management of Risk—Principles and Concepts* (updated 2026)

Information Commissioner's Office, 'Data protection by design and by default' https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-by-default/ accessed 5 August 2026

Information Commissioner's Office, 'Guidance on AI and data protection' https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ accessed 5 August 2026

Information Commissioner's Office, 'Privacy-enhancing technologies' https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/ accessed 5 August 2026

International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) UN Doc A/56/10

ISO 22301:2019, *Security and Resilience—Business Continuity Management Systems—Requirements*, as amended by ISO 22301:2019/Amd 1:2024

ISO/IEC 11770-1:2010, *Information Technology—Security Techniques—Key Management—Part 1: Framework*

ISO/IEC 19941:2017, *Cloud Computing—Interoperability and Portability*

ISO/IEC 27037:2012, *Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*

ISO/IEC 27041:2015, *Guidance on Assuring Suitability and Adequacy of Incident Investigative Methods*

ISO/IEC 27042:2015, *Guidelines for the Analysis and Interpretation of Digital Evidence*

ISO/IEC 27043:2015, *Incident Investigation Principles and Processes*

John Kelsey, Jon Callas and Anton Clemm, 'Signed Syslog Messages' (RFC 5848, May 2010)

Linux Foundation, *SPDX Specification 2.3* (2022)

Michael Jones, John Bradley and Nat Sakimura, 'JSON Web Token (JWT)' (RFC 7519, May 2015)

Michael Jones, Nat Sakimura and John Bradley, 'OAuth 2.0 Authorization Server Metadata' (RFC 8414, June 2018)

MISP Project, 'MISP Standard' https://www.misp-standard.org/ accessed 5 August 2026

MITRE, 'ATT&CK' https://attack.mitre.org/ accessed 5 August 2026

National Audit Office, *Digital Transformation in Government: Addressing the Barriers to Efficiency* (10 March 2023)

National Audit Office, *Government's Approach to Technology Suppliers: Addressing the Challenges* (16 January 2025)

National Cyber Security Centre, 'Cloud-hosted SCADA' https://www.ncsc.gov.uk/collection/operational-technology/cloud-hosted-scada accessed 5 August 2026

National Cyber Security Centre, 'Cyber Assessment Framework' https://www.ncsc.gov.uk/collection/caf accessed 5 August 2026

National Cyber Security Centre, 'Introduction to logging for security purposes' (8 July 2018) https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes accessed 5 August 2026

National Cyber Security Centre, 'Logging Made Easy' (updated 18 September 2025) https://www.ncsc.gov.uk/information/logging-made-easy accessed 5 August 2026

National Cyber Security Centre, 'Secure design principles' https://www.ncsc.gov.uk/collection/cyber-security-design-principles accessed 5 August 2026

National Cyber Security Centre, 'The cloud security principles' https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles accessed 5 August 2026

National Cyber Security Centre, 'Zero trust architecture design principles' (16 January 2026) https://www.ncsc.gov.uk/collection/zero-trust/architecture-design-principles accessed 5 August 2026

National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1, 2023)

National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information Systems* (NIST SP 800-34 rev 1, 2010)

National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (NIST SP 800-161 rev 1, 2022)

National Institute of Standards and Technology, *Digital Identity Guidelines: Authentication and Authenticator Management* (NIST SP 800-63B-4, 2025)

National Institute of Standards and Technology, *Digital Identity Guidelines: Federation and Assertions* (NIST SP 800-63C-4, 2025)

National Institute of Standards and Technology, *Digital Identity Guidelines: Identity Proofing and Enrollment* (NIST SP 800-63A-4, 2025)

National Institute of Standards and Technology, *Digital Identity Guidelines* (NIST SP 800-63-4, 2025)

National Institute of Standards and Technology, *Guide for Conducting Risk Assessments* (NIST SP 800-30 rev 1, 2012)

National Institute of Standards and Technology, *Guide to Computer Security Log Management* (NIST SP 800-92, 2006)

National Institute of Standards and Technology, *Guide to Data-Centric System Threat Modeling* (initial public draft, NIST SP 800-154, 2016)

National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response* (NIST SP 800-86, 2006)

National Institute of Standards and Technology, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management* (NIST SP 800-61 rev 3, 2025)

National Institute of Standards and Technology, *NIST Cloud Computing Forensic Reference Architecture* (NIST SP 800-201, 2024)

National Institute of Standards and Technology, *NIST Cloud Computing Forensic Science Challenges* (NISTIR 8006, 2014)

National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0* (2020)

National Institute of Standards and Technology, *Recommendation for Key Management: Part 1—General* (NIST SP 800-57 pt 1 rev 5, 2020)

National Institute of Standards and Technology, *Secure Software Development Framework (SSDF) Version 1.1* (NIST SP 800-218, 2022)

National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53 rev 5, 2020, updated 2020)

National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules* (FIPS 140-3, 2019)

National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29, 2024)

National Telecommunications and Information Administration, *The Minimum Elements for a Software Bill of Materials* (12 July 2021)

Network and Information Systems Regulations 2018, SI 2018/506

OASIS Open, *STIX Version 2.1* (OASIS Standard, 10 June 2021) https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html accessed 5 August 2026

OASIS Open, *TAXII Version 2.1* (OASIS Standard, 10 June 2021) https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html accessed 5 August 2026

OpenCTI, ‘OpenCTI Documentation’ https://docs.opencti.io/ accessed 5 August 2026

OWASP Foundation, *CycloneDX Specification 1.6* (2024)

Rainer Gerhards, ‘The Syslog Protocol’ (RFC 5424, March 2009)

Scott Rose and others, *Zero Trust Architecture* (NIST SP 800-207, National Institute of Standards and Technology 2020) 4–7 https://doi.org/10.6028/NIST.SP.800-207 accessed 5 August 2026

SLSA, *Supply-chain Levels for Software Artifacts Specification v1.0* (2023)

US Department of Justice, *The Purpose and Impact of the CLOUD Act* (April 2019)

World Wide Web Consortium, *PROV-O: The PROV Ontology* (W3C Recommendation, 30 April 2013)

1. From Doctrine to an Operating Service

A doctrine which says that States should cooperate is correct but incomplete. The packet has passed, the workload has ended and the log has been deleted before a diplomatic note is translated. A provider receiving an urgent request cannot authenticate the sender; a national authority cannot know whether the indicator appears elsewhere; counsel cannot tell whether a match is a forensic observation, an intelligence assessment or the output of a model; and a court receives a spreadsheet whose provenance began after the incident rather than at collection. The failure is not invariably unwillingness. Frequently there is no common instrument by which willing actors can move at the speed of the evidence.

MOSAIC is intended to be that instrument. Its full name identifies its limits. It correlates *signals*, because an indicator or event is evidence from which propositions may be inferred and is not itself attribution. It protects *integrity*, because speed without provenance creates a swift means of manufacturing error. It operates across *jurisdictions*, because evidence remains subject to the law of the custodian and is not silently drawn into a British repository. It supports *attribution*, because the final legal and political judgement remains with the competent authority.

The service has six objectives. First, an authenticated emergency preservation notice should reach the correct custodian in minutes, not months. Secondly, a national node should be able to discover that the same operation identifier, infrastructure, credential artefact or behavioural sequence appears in other territories without obtaining all underlying personal data. Thirdly, every assertion should disclose its source class, time, confidence, transformation and custodian. Fourthly, the controller of a State or PMSC operation should be capable of lodging a sealed attribution manifest which records the human authority and technical composition without exposing it during legitimate operations. Fifthly, the system should produce material which can survive judicial challenge, including proof of collection, transformation and access. Sixthly, error should be correctable throughout the federation rather than copied permanently.

These objectives distinguish MOSAIC from a threat-intelligence feed. A feed distributes indicators so recipients may defend themselves. MOSAIC also does that where appropriate, but its distinctive functions are lawful discovery, preservation and evidential continuity. Nor is it a mutual legal assistance treaty in software. It does not replace judicial authority or the terms upon which evidence may be produced. It supplies the rapid preliminary acts and common record which make later process useful.

The design should be judged against four propositions developed in Paper 3. A territorial fragment is not the whole operation; due diligence concerns what the particular State knew and could reasonably do; the principal correlation duty belongs to the actor which possessed the operation map; and intentional fragmentation must not enable that actor to obtain the evidential benefit of its own design. Each proposition has a software consequence. Local custody answers the first. Notice, capacity and action logs answer the second. The manifest answers the third. Signed correlation and spoliation records answer the fourth.[1]

There is a political consequence also. A federation which can be used only against disfavoured States will not become a rule. The same interface by which the United Kingdom asks an ally to preserve evidence must permit that ally to make a properly authorised request of the United Kingdom. Reciprocity need not mean identical access where legal systems differ; it requires a published basis for difference, review and a refusal reason capable of audit. Power which operates only in one direction is not cooperation. It is dependence.

[1] Evelyne Schmid and Ayşe Özge Erceiş, ‘The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility’ (2023) 33 *Swiss Review of International and European Law* 577, 581–90.

1.1 Design Principles

The first principle is local custody. Except where lawfully produced, raw content and identifying logs remain with the organisation which already holds them. A national node maintains indexes, signed receipts and disclosed results; it does not ingest every participant's telemetry. This reduces the attraction of the central service as a target and respects legal restrictions upon transfer.

The second is minimum necessary disclosure. Discovery ordinarily begins with a pseudonymous or cryptographically transformed query. A responder may return "match", time band, evidence class and confidence before identity or content. Disclosure increases only when urgency, legal authority and proportionality require it. Privacy is thereby made part of the workflow rather than a promise appended after construction.

The third is evidential separation. An observed event, a provider record, a technical inference, an intelligence assessment and a State attribution must never be flattened into one field called "fact". A proposition carries its class, author, method and confidence. Where a model assisted, its output is recorded as analysis; the underlying observations remain available subject to law.

The fourth is cryptographic accountability. Nodes, gateways and authorised persons sign what they submit. Time is obtained from resilient trusted sources. Transformations are reproducible or described. Deletion, correction and supersession do not erase the audit history, although access to personal data may be restricted or the data destroyed where law requires.

The fifth is no implicit trust. A friendly national node is not trusted merely because its network is allied. Every session, service and request is authenticated and authorised for its particular purpose. NIST's zero-trust architecture gives the correct general proposition: network location or ownership does not itself confer trust.[2] Diplomatic status is relevant to policy; it is not a substitute for technical verification.

The sixth is graceful refusal. A State or provider unable lawfully to answer should return a signed reason class—no match, insufficient particularity, no authority, conflicting law, privilege, disproportionate burden, national security, technical incapacity or suspected abuse—without disclosing protected material. Silence destroys both urgency and later evaluation of due diligence.

The seventh is open interchange, replaceable components and public specification. The United Kingdom should not create permanent dependence upon one supplier for a sovereign evidential service. Source code need not all be public where disclosure would create a vulnerability, but schemas, protocols, conformance tests and export formats should be.

The eighth is human responsibility. Automation may route, normalise, match, deduplicate and prioritise. It must not itself issue a coercive production order, accuse a person or determine that a foreign State committed an internationally wrongful act. The system should make the responsible human visible, not hide him behind an automated score.

1.2 What MOSAIC Does Not Claim

An IP address does not identify an attacker. A certificate, domain, tool or model fingerprint may be shared, stolen or planted. A correlation is not causation; common infrastructure is not common command; State affiliation is not article 8 control. MOSAIC must make weak evidence faster without making it appear strong.

[2] Scott Rose and others, *Zero Trust Architecture* (NIST SP 800-207, National Institute of Standards and Technology 2020) 4–7 https://doi.org/10.6028/NIST.SP.800-207 accessed 5 August 2026; National Cyber Security Centre, 'Zero trust architecture design principles' (16 January 2026) https://www.ncsc.gov.uk/collection/zero-trust/architecture-design-principles accessed 5 August 2026; Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model Version 2.0* (April 2023).

The protocol does not grant extraterritorial jurisdiction. A British request delivered to a provider in another State has only the force supplied by that State's law, an applicable agreement or the provider's lawful voluntary power. Where the Second Additional Protocol to the Budapest Convention, the European electronic-evidence regime, a CLOUD Act executive agreement, mutual assistance, emergency cooperation or domestic production law applies, MOSAIC can carry the authenticated record and relevant metadata; it cannot enlarge the instrument.[3]

Nor does it compel decryption which a provider cannot perform, place a universal backdoor in lawful services, or require indiscriminate retention. It preserves identified evidence and allows risk-tiered security logging where legislation supplies a basis. Data minimisation and evidential sufficiency must be reconciled in the system design.

Finally, the protocol cannot decide whether a cyber operation constitutes intervention, a use of force or an armed attack. It can assemble scale, effects, target, duration and consequences in a structured form. The victim State must apply international law, including necessity and proportionality, to a record which remains open to contradiction.

1.3 Operational Assumptions and Acceptance Tests

The design proceeds upon adverse assumptions, for a public service which is safe only whilst every participant behaves honourably is merely an arrangement for sharing the consequences of dishonour. One partner node will eventually be compromised; one custodian will have a clock which has drifted; one provider will interpret a field differently; one urgent request will contain an innocent identifier; one minister will prefer a confident conclusion to a qualified one; one supplier will cease trading or seek to make replacement prohibitively expensive; and an adversary will observe the protocol sufficiently well to route around participating jurisdictions. NIST risk-assessment and data-centric threat-modelling guidance support the discipline of stating assets, threat sources, attack paths and assumptions before selecting controls, whilst the NCSC's secure-design principles require an architecture to make compromise difficult, detectable and recoverable.[4]

The principal assets are not confined to evidence. They include the secrecy of an investigation; the integrity of the trust registry; the relation between a query and the authority for it; the identity of a protected subject; the ordering of events; the fact that a jurisdiction did or did not possess knowledge; the software and policy version which made a decision; and the availability of the emergency route before an ordinary retention period expires. Each asset has a different owner and consequence. The loss of a pseudonymous indicator may be modest; alteration of a signed refusal may manufacture the appearance that a State ignored notice; theft of the query graph may disclose the blind spots of an alliance.

Accordingly, acceptance is stated as propositions capable of failure. A four-node pilot must continue safe routing after one node is quarantined. A signed object must remain verifiable after ordinary key rotation and must be identified for revalidation after an asserted compromise. A correction must reach

[3] Convention on Cybercrime (opened for signature 23 November 2001, entered into force 1 July 2004) ETS No 185; Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (opened for signature 12 May 2022) CETS No 224; Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191/118; Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on designated establishments and legal representatives for gathering electronic evidence in criminal proceedings [2023] OJ L191/181; Clarifying Lawful Overseas Use of Data Act 2018, Pub L No 115-141, div V, 132 Stat 1213; Crime (Overseas Production Orders) Act 2019.

[4] National Institute of Standards and Technology, *Guide for Conducting Risk Assessments* (NIST SP 800-30 rev 1, 2012); National Institute of Standards and Technology, *Guide to Data-Centric System Threat Modeling* (initial public draft, NIST SP 800-154, 2016); National Cyber Security Centre, 'Secure design principles' https://www.ncsc.gov.uk/collection/cyber-security-design-principles accessed 5 August 2026.

every recorded recipient, even if one was offline when it issued. A provider must be able to prove that it preserved a defined record without disclosing the record to the federation. An analyst must be unable to convert a similarity result into a legal attribution merely by changing a display field. A legal reviewer must be able to reconstruct the authority, purpose and territorial route without assistance from the developer who wrote the workflow.

Performance must also be tested against the hostile case, not solely the median. The service target concerns the ninety-fifth percentile and the expiring record; capacity testing includes a malicious flood; privacy testing includes enumeration of small input domains; accessibility testing includes the duty officer under fatigue; and evidential testing begins with an advocate instructed to challenge the record. The NIST Cybersecurity Framework 2.0 and incident-response guidance treat governance, detection, response and recovery as connected outcomes, whilst the NCSC Cyber Assessment Framework asks whether essential functions remain protected and resilient rather than whether a product has acquired a certificate.[5]

There are, finally, three propositions upon which the pilot must be willing to stop. If the same evidential benefit can be obtained by improving existing bilateral channels at materially lower cost, MOSAIC is unnecessary. If privacy-preserving discovery cannot resist practical enumeration without latency which defeats preservation, that function must be narrowed. If partners will exchange indicators but will not accept reciprocal audit, correction and suspension, the proposed federation would increase confidence more readily than truth. A feasibility exercise which discovers any of these matters has not failed. It has prevented doctrine from hardening into an expensive constitutional mistake.

2. The System to Be Built

MOSAIC consists of four planes: custody, federation, decision and oversight. The custody plane is formed by provider and public-authority gateways which hold or address evidence. The federation plane routes signed discovery and preservation messages amongst national nodes. The decision plane is the legally competent human machinery which approves requests, production, disruption and public attribution. The oversight plane inspects use, security, refusals, correction and systemic bias.

[5] National Institute of Standards and Technology, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management* (NIST SP 800-61 rev 3, 2025); National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29, 2024); National Cyber Security Centre, ‘Cyber Assessment Framework’ https://www.ncsc.gov.uk/collection/caf accessed 5 August 2026.

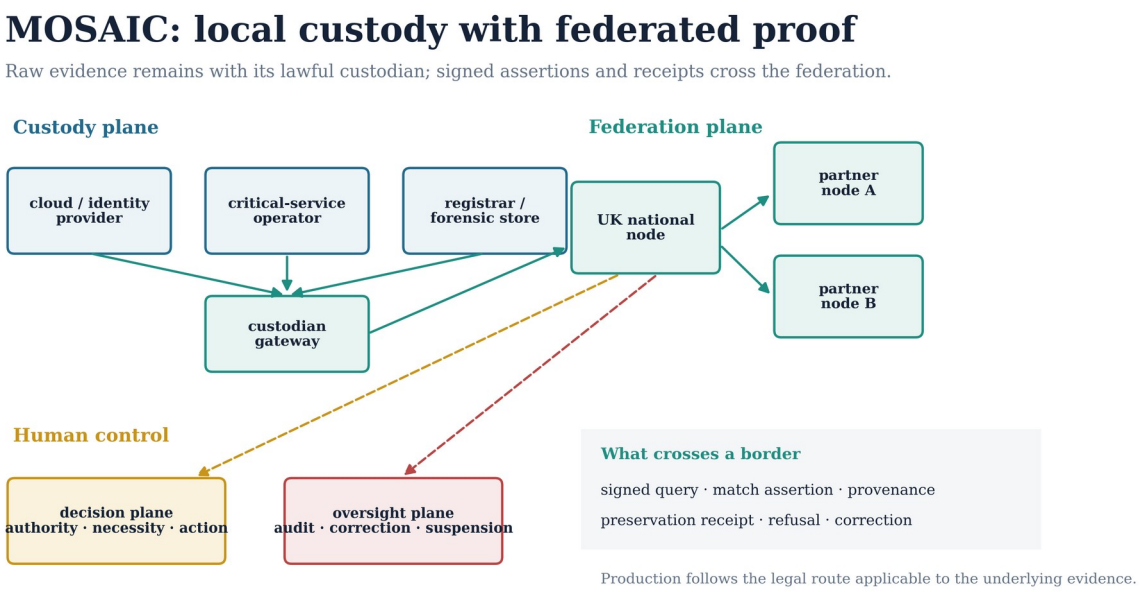

Figure 1. MOSAIC architecture: local evidence custodians connect through national nodes; national nodes federate signed queries; decision and oversight remain outside the automated correlation plane.

No central international server is required. Each participating State operates a national node under its own law and appoints a competent authority. Nodes maintain a trust registry containing public keys, service endpoints, authority scope, emergency contacts and current suspension status. A multilateral governance body publishes the common protocol and conformance tests, but need not possess operational evidence.

Within the United Kingdom the national node should be technically operated by, or under the security authority of, the National Cyber Security Centre, whilst legal gateways distinguish functions. NCSC may coordinate national technical response; the National Crime Agency may seek criminal evidence; the Information Commissioner may supervise personal-data processing; sector regulators may act upon regulated entities; police and prosecutors may proceed under their own powers; and ministers may receive an attribution package for public and international response. One database which makes these constitutional distinctions invisible would be efficient only in the sense that error is efficient.

2.1 Custodian Gateway

A custodian gateway is a small service or managed connector deployed by a provider, operator of essential services, registrar, exchange, public body or forensic laboratory. It maps the custodian’s logs to the common schema, maintains a local encrypted index, receives authorised queries and returns the minimum permitted result. Small organisations may use a hosted gateway operated by an accredited service, but the host should not receive decryption keys for raw evidence unless separately authorised.

The gateway requires connectors for common log sources: identity and access management; domain registration; cloud control plane; workload execution; network flow; endpoint detection; email; payment reference; software build and model-agent audit; and preservation status. It should not require a provider to retain content it does not ordinarily possess. It records what is absent as carefully as what is present.

Normalisation occurs locally. An IP observation, for example, is not stored merely as a string. It carries observation time and uncertainty, source sensor, direction, protocol, network address translation context where known, collection clock status, processing steps, legal basis, retention expiry and sensitivity. A

domain record distinguishes creation, resolution, access and analytic association. A model execution distinguishes objective, tool permission, human approval and actual action.

The gateway may answer three query classes. An exact query asks whether a precise normalised value occurred within a time band. A similarity query asks whether a behavioural sequence or privacy-preserving representation passes a published threshold. An operation query asks whether the custodian has records bearing a signed operation identifier issued by a controller or investigator. Similarity carries the greatest risk of false association and therefore returns a candidate for human review, never an attribution.

The local index may employ keyed hashes, private set intersection or another assessed privacy-enhancing technique so that ordinary discovery does not expose raw identifiers. The Information Commissioner's guidance recognises that privacy-enhancing technologies may support data minimisation and secure data sharing, but their suitability depends upon purpose, implementation and residual risk.[6] Private set-intersection research demonstrates the relevant possibility—the parties may discover common elements without disclosing every non-matching element—but deployment security depends upon protocol, implementation and the domain being queried.[7] A hash of a small predictable value is not anonymity; it may be reversed by enumeration. Keys, salts, rate limits and query auditing are essential.

2.2 National Node

The national node is a router, policy enforcement point, receipt store and correlation workbench. It authenticates the requesting authority; verifies whether the requested action falls within its accredited role; checks purpose, urgency and particularity; applies the sending State's disclosure policy; and routes to other nodes according to bilateral or multilateral rules.

The node does not allow an analyst to search every foreign dataset as if it were one domestic warehouse. A query is submitted as a case-bound request. It receives a unique request identifier, names the legal or voluntary basis, defines a time window, specifies permitted responders, states whether the subject may be notified and records the authorising person. Queries which concern journalists, lawyers, parliamentarians, political parties or protected civil-society activity receive enhanced review because the same mechanism which detects hostile reconnaissance may be abused to map lawful opposition.

A correlation workbench assembles replies into a graph. It displays source class and confidence upon every edge. It does not visually merge "observed from address", "controlled account", "same malware", "paid invoice", "received State tasking" and "legally attributable". An analyst may see that five fragments align temporally whilst three have plausible innocent explanations. Contradictions remain visible.

The receipt store retains signed notices, acknowledgements, preservation states, refusals, supersessions and access logs. It need not contain the underlying evidence. A receipt proves that a statement was made and received at a time; it does not prove the truth of the underlying accusation.

[6] Information Commissioner's Office, 'Privacy-enhancing technologies' https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/ accessed 5 August 2026; National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0* (2020); European Union Agency for Cybersecurity, *Pseudonymisation Techniques and Best Practices* (ENISA 2019).

[7] Lea Kissner and Dawn Song, 'Privacy-Preserving Set Operations' in Victor Shoup (ed), *Advances in Cryptology—CRYPTO 2005* (Springer 2005) 241; Michael Freedman, Kobbi Nissim and Benny Pinkas, 'Efficient Private Matching and Set Intersection' in Christian Cachin and Jan Camenisch (eds), *Advances in Cryptology—EUROCRYPT 2004* (Springer 2004) 1; Benny Pinkas, Thomas Schneider and Michael Zohner, 'Faster Private Set Intersection Based on OT Extension' (23rd USENIX Security Symposium 2014) 797.

The node also manages emergency priority. Imminent danger to life, active compromise of critical national infrastructure, election integrity and destructive attacks may receive a short decision target. Commercial loss without systemic effect remains serious but should not automatically displace life-safety incidents. Priority is reviewable and recorded.

2.3 Federation Layer

National nodes communicate through mutually authenticated channels using a common message envelope. TAXII 2.1 is an application-layer protocol for exchanging cyber-threat information and STIX 2.1 supplies a language and serialisation format for threat and observable information.[8] They are a sensible base because tools and expertise already exist and because cooperative information-sharing models provide practical evidence concerning trust, governance and operational maturity.[9] They do not, without extension, supply the legal authority, evidential provenance, preservation state, purpose restriction, refusal, challenge or manifest required here.

MOSAIC therefore defines additional signed objects:

- **Case Object**: case identifier, competent authority, purpose, legal basis, protected interest and handling classification.
- **Signal Object**: normalised observation or query value, time uncertainty, source class, confidence, transform and sensitivity.
- **Preservation Object**: scope, custodian, expiry, legal basis, status, receipt and subsequent production route.
- **Authority Object**: identity, role, jurisdiction, permitted actions, warrant or approval reference and revocation.
- **Manifest Object**: controller, objective, authorising human, model or software versions, infrastructure map, subcontractors, constraints and sealed-access conditions.
- **Inference Object**: proposition, inputs, method, analyst or model, confidence, alternatives and validation.
- **Correction Object**: contested item, reason, disposition, propagation status and effect upon prior assessments.
- **Refusal Object**: reason class, reviewing authority, lawful alternative and urgency response.

Each object is versioned and signed. Common fields use controlled vocabularies; national extensions remain possible but cannot silently change the meaning of a required field. Conformance testing verifies syntax, cryptography, state transition and refusal handling rather than merely the ability to exchange a sample.

Federation is governed by trust tiers. A full partner may issue and answer discovery and preservation requests under a binding instrument. A limited partner may exchange defensive indicators but not personal-data matches. An emergency contact may receive a life-safety preservation notice pending formal process. A suspended node may receive public warnings but cannot query. Trust can be reduced without dismantling the network.

---

[8] OASIS Open, *STIX Version 2.1* (OASIS Standard, 10 June 2021) https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html accessed 5 August 2026; OASIS Open, *TAXII Version 2.1* (OASIS Standard, 10 June 2021) https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html accessed 5 August 2026; MISP Project, 'MISP Standard' https://www.misp-standard.org/ accessed 5 August 2026; OpenCTI, 'OpenCTI Documentation' https://docs.opencti.io/ accessed 5 August 2026; MITRE, 'ATT&CK' https://attack.mitre.org/ accessed 5 August 2026.

[9] Sarah Brown, Joep Gommers and Oscar Serrano, 'From Cyber Security Information Sharing to Threat Management' in WISCS '15: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security* (ACM 2015) 43, 43–49; European Union Agency for Cybersecurity, *Cooperative Models for Information Sharing and Analysis Centres* (ENISA 2018); Forum of Incident Response and Security Teams, *Traffic Light Protocol (TLP): FIRST Standards Definitions and Usage Guidance—Version 2.0* (2022).

2.4 Decision Plane

Every consequential action has a named decision owner. A service operator may approve a defensive exact-match query; an emergency duty officer may authorise temporary preservation under statutory criteria; a court or designated authority may order production; an operator may isolate its own compromised system; ministers or authorised officials may impose sanctions or make a public attribution; military decisions remain entirely outside MOSAIC and subject to their own law and command.

The system presents a decision record which includes what is known, what is inferred, confidence, contrary explanations, likely expiry, available measures and collateral implications. It should not present a single composite “attribution score”. Such a score would conceal the difference between technical linkage, identity, control, intent and legal responsibility.

Urgency alters sequence, not accountability. An emergency preservation may precede full judicial review because it freezes rather than discloses; it should expire unless confirmed. A temporary defensive block upon a government network may be immediate; coercive action against a foreign person requires the authority applicable to it. The decision log allows ex post review to occur upon an unaltered record.

2.5 Oversight Plane

Independent oversight must have technical access sufficient to test use without acquiring operational control. In the United Kingdom this requires a statutory commissioner or a defined expansion of an existing office, supported by security-cleared technical and legal staff. The overseer should inspect samples, emergency use, protected-category queries, refusals, error correction, retention, model performance and security incidents.

Aggregate transparency reports should disclose the number and kind of queries, States involved, emergency authorisations, matches, preservation requests, production orders, refusals, corrections, security events and disciplinary findings. Counts may be delayed or banded where immediate publication would expose operations. Secrecy should protect an operation; it should not prevent the public from discovering whether a permanent system is habitually used outside its purpose.

Parliament should receive a classified annex and a public annual report. Courts and affected persons require routes to challenge unlawfully obtained or inaccurate material where notice is compatible with the investigation. A correction entered in one node should propagate to every recipient of the original object, together with notice of any materially affected conclusion.

2.6 Trust Registry, Message Integrity and Time

The trust registry is the constitutional address book of the federation. For each human authority, service and node it records the issuing jurisdiction, public key, permitted roles, legal instruments upon which those roles depend, protected categories which require additional approval, technical conformance version, security contact, commencement, expiry and suspension. It is not enough that a certificate says “United Kingdom”: the recipient must know whether its holder may send a defensive indicator, request preservation, certify a production order or open a manifest. Digital identity guidance distinguishes identity proofing, authentication and federation because a strong authenticator cannot cure the enrolment of the wrong person or an excessive grant of authority.[10]

[10] National Institute of Standards and Technology, *Digital Identity Guidelines* (NIST SP 800-63-4, 2025); National Institute of Standards and Technology, *Digital Identity Guidelines: Identity Proofing and Enrollment* (NIST SP 800-63A-4, 2025); National Institute of Standards and Technology, *Digital Identity Guidelines: Authentication and Authenticator Management* (NIST SP 800-63B-4, 2025); National Institute of Standards and Technology, *Digital Identity Guidelines: Federation and*

Authority objects are short-lived and constrained. A national root delegates to operational issuers; an issuer delegates a role to a service or official; the message carries the relevant chain and the recipient checks revocation, purpose, audience and time. Mutual TLS protects the session, but the application object is signed independently so that it can be stored, forwarded and proved after the transport connection has ended. Current IETF standards supply suitable elements: TLS 1.3 for transport, mutual-TLS client authentication where appropriate, HTTP Message Signatures for selected request components, and CBOR Object Signing and Encryption for compact signed objects.[11] MOSAIC specifies profiles, permissible algorithms and canonical serialisation; it does not invite every node to assemble an untested cryptographic mixture.

The message envelope contains an object identifier, case identifier, sender, recipient class, created time, expiry, nonce, sequence, schema version, policy version, content digest and signature. A receiving node rejects an expired message, a replayed nonce, a sequence outside its allowed window, a signature under a suspended key and a mandatory field whose meaning it does not support. It may accept an older schema only through a published compatibility rule. JSON Web Tokens and general OAuth deployments are not, by their names, evidence protocols; their threat models, audience restriction and bearer-token risks must be addressed, and the more recent OAuth security practice must displace deprecated flows.[12]

Time is evidence and also an attack surface. RFC 3339 supplies a common representation; the Time-Stamp Protocol can attest that a digest existed by a particular time; signed syslog and transparency-log designs illustrate sequencing, detection of missing entries and append-only verification.[13] None proves that an originating sensor’s wall clock was correct. MOSAIC therefore stores event time, ingestion time, signing time, trusted timestamp, clock source, last synchronisation and uncertainty separately. Where a camera, industrial controller or edge device has no trustworthy clock, the record says so and uses correlation bounds rather than inventing a precise second.

The audit store uses hash-linked batches and independent witnessing. At defined intervals a node commits a digest of its receipt log to at least two separately administered witnesses. A later investigator can prove inclusion and detect divergent histories without publishing live content. Certificate Transparency demonstrates both the utility of Merkle-tree proofs and the danger that a dishonest log may show inconsistent views; MOSAIC therefore requires cross-node gossip or equivalent consistency checking and does not treat an append-only claim as self-authenticating.[14]

Cryptographic agility is governed, not improvised. The security authority publishes an algorithm schedule, minimum key protection, migration period and emergency deprecation process, drawing upon NIST key-management guidance and validated cryptographic-module standards.[15] A broken primitive triggers re-signing and re-witnessing of surviving records where possible; it does not silently erase their

Assertions (NIST SP 800-63C-4, 2025).

[11] Eric Rescorla, ‘The Transport Layer Security (TLS) Protocol Version 1.3’ (RFC 8446, August 2018); Brian Campbell and others, ‘OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens’ (RFC 8705, February 2020); Annabelle Backman and others, ‘HTTP Message Signatures’ (RFC 9421, February 2024); Jim Schaad, ‘CBOR Object Signing and Encryption (COSE): Structures and Process’ (RFC 9052, August 2022).

[12] Michael Jones, John Bradley and Nat Sakimura, ‘JSON Web Token (JWT)’ (RFC 7519, May 2015); Torsten Lodderstedt, John Bradley, Andrey Labunets and Daniel Fett, ‘Best Current Practice for OAuth 2.0 Security’ (RFC 9700, January 2025); Michael Jones, Nat Sakimura and John Bradley, ‘OAuth 2.0 Authorization Server Metadata’ (RFC 8414, June 2018).

[13] Graham Klyne and Chris Newman, ‘Date and Time on the Internet: Timestamps’ (RFC 3339, July 2002); Carlisle Adams and others, ‘Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)’ (RFC 3161, August 2001); Rainer Gerhards, ‘The Syslog Protocol’ (RFC 5424, March 2009); John Kelsey, Jon Callas and Anton Clemm, ‘Signed Syslog Messages’ (RFC 5848, May 2010).

[14] Ben Laurie, Emilia Messeri and Rob Stradling, ‘Certificate Transparency Version 2.0’ (RFC 9162, December 2021).

[15] National Institute of Standards and Technology, *Recommendation for Key Management: Part 1—General* (NIST SP 800-57 pt 1 rev 5, 2020); National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules* (FIPS 140-3, 2019); ISO/IEC 11770-1:2010, *Information Technology—Security Techniques—Key Management—Part 1: Framework*.

earlier status. Historic verification packages retain the certificate chain, revocation material, timestamp and policy by which a signature was assessed at the relevant time.

Trust has to degrade safely. Evidence signed before a node's compromise is neither automatically true nor automatically useless. The incident record identifies the suspected interval, keys, services and object classes; recipients quarantine affected inferences, seek confirmation from original custodians, and preserve the former decision state. New queries from the node cease at once. Emergency warnings may continue through an out-of-band contact because suspension of authority should not prevent a compromised State from warning others that an attack is in progress.

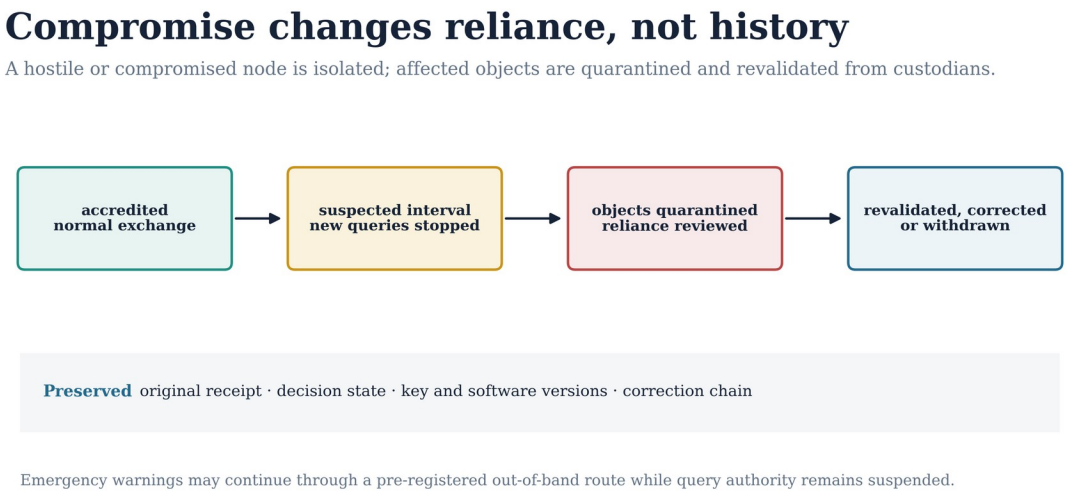

Figure 2. Compromise response: authority is suspended, affected objects are quarantined and original decision history is retained whilst revalidation proceeds.

3. The Common Evidential Model

Cyber investigations fail as readily from incompatible meaning as from absent data. One provider's "creation time" is another's first ingestion; one analyst's "confirmed" means forensic observation, another's high-confidence inference; one State's "APT31" refers to a cluster, another's to a public attribution. MOSAIC requires a semantic contract.

The minimum event record contains:

1. a globally unique event identifier and the identifier assigned by its custodian;
2. observation start and end, clock source, time zone and uncertainty;
3. event type and schema version;
4. originating system, sensor class and collection method;
5. normalised values and the unaltered source reference;
6. transformation history, including parsing, filtering, enrichment and model use;
7. collector identity and signature where available;
8. custodian, territorial location and control location where known;
9. legal basis, purpose limitation and handling restriction;
10. retention expiry and preservation state;
11. confidence and source class;
12. links to corrections, challenges and later production.

This list is not an instruction to collect every field from every person. It is the form in which a field, if collected and relied upon, should be understood. A provider which never records content states “not collected”; one unable to determine physical data location states “distributed or unknown”. Honest absence is preferable to a false precision introduced by normalisation.

3.1 Source Classes

The following source classes are mandatory:

- **direct observation**: generated by a sensor or system record whose operation is described;
- **custodian record**: account, subscriber, payment or service record maintained in ordinary business;
- **forensic finding**: derived through a documented examination;
- **human statement**: witness, suspect, operator or official account;
- **technical inference**: analytic linkage from observations;
- **intelligence assessment**: assessment whose full basis may be protected;
- **model-assisted analysis**: output materially produced by a computational model;
- **legal finding**: proposition determined by a competent court or tribunal;
- **State position**: public or protected attribution or legal position of a State;
- **third-party report**: journalism, civil-society, academic or commercial report not otherwise classified.

A proposition may rest upon several classes. The system records each path. An indictment is a legal document proving that allegations were made and charges brought; it is not a finding of guilt. A government attribution proves the State’s position and disclosed basis; it is not transformed into a judgment. The distinction which protects forceful scholarship also protects public action.

3.2 Confidence and Contrary Hypotheses

Confidence is stated separately for observation authenticity, technical linkage, identity, common operation, direction or control, intent and legal character. A high-confidence match between two hashes says nothing by itself about State responsibility. An analyst must state the inference and the alternative explanations considered: shared service, recycled code, deception, compromised infrastructure, coincidence, independent use or error.

MOSAIC should use verbal confidence bands accompanied by defined probability ranges only where the participating authority already employs them and their meaning is displayed. False mathematical precision is dangerous, but undefined phrases are worse. A decision maker must know whether “likely” means more probable than not or merely plausible.

Where a model recommends a link, the record identifies model and version, input features available to it, threshold, validation set, known limitations and human reviewer. Sensitive model details may be protected from an attacker, but the defence or reviewing court may require enough information to test reliability. A model cannot improve weak provenance by processing it.

3.3 The Attribution Manifest

The attribution manifest is the distinguishing controller-side instrument. A State body, PMSC or designated high-risk autonomous operator records, before or during deployment, the following:

- the lawful objective and authorising person;
- the entity responsible for operational control;

- expected target classes and prohibited targets;
- software, model and tool versions;
- accounts, providers and jurisdictions expected to be used;
- prime and subcontractors, with task boundaries;
- credentials and signing identities;
- human approval points and automated discretion;
- constraints, stop conditions and change authority;
- logs and retention;
- material deviations, incidents and termination.

The manifest may be encrypted and divided amongst independent custodians so that no single official can reveal a legitimate covert operation. Access conditions may require two or more authorised officers, a court, an inspector, a specified incident threshold or later declassification. What matters is that the controller cannot plausibly claim after severe harm that no operation map ever existed.

The manifest is not a licence. Recording an unlawful objective does not make it lawful. Nor should its mere existence be visible to ordinary foreign queries. It is a sealed accountability record, available under national law and applicable international process. Failure to create it, or intentional destruction after a duty to preserve, may support regulatory sanction and an adverse inference in proceedings appropriate to the applicable standard of proof.

A software-generated manifest is insufficient unless a human authority attests to objective and constraints. Conversely, requiring a minister to understand every container and library is absurd. The document has levels: strategic authority, operational design, technical bill of materials and event amendments. Each is signed by the person responsible for that level.

3.4 Chain of Custody

Evidence should be hashed at collection or first admission, signed where the source supports it and placed in append-only storage. Every transformation creates a new object linked to its parent. Access, export and production are logged. Trusted timestamps are obtained from several sources and clock drift recorded.

Append-only does not mean immortal. Personal data may have to be erased. MOSAIC separates the audit fact that an object existed and was lawfully deleted from the content itself. A tombstone retains identifier, authority and time without retaining the deleted personal data. Where litigation hold or preservation law applies, the conflict is determined before erasure and recorded.

For court production the custodian exports the underlying record, schema, transformation history, relevant software version, hash, signatures, access log and witness statement or certificate required by domestic procedure. The national node supplies routing and receipt records. Counsel can then distinguish authenticity, hearsay, expert opinion, privilege and weight.

3.5 Correction, Challenge and Contamination

Indicators are frequently wrong or cease to be useful. An address is reassigned; a domain is sinkholed; a tool becomes public; an innocent account is compromised. If an incorrect association travels through twelve nodes, merely correcting the originating dashboard does not repair it.

A correction object identifies the original, reason, evidence, authorised decision and affected downstream conclusions. Nodes must acknowledge propagation. Where an earlier attribution package

materially relied upon the item, the system flags it for reassessment. The audit retains the former state so that investigators cannot conceal that an action was taken upon mistaken evidence.

An affected provider or person may submit a challenge through the competent national authority, subject to security restrictions. The process need not reveal an active investigation, but it must permit error to be tested eventually. Bad-faith challenges and flooding are rate-limited; lawful challenge is not treated as hostility.

Evidence may be contaminated by a compromised node. Trust revocation must identify every object signed by the node during the suspected interval, suspend automated reliance and require revalidation from original custodians where possible. The federation assumes compromise will occur. Its purpose is to contain it without destroying all prior evidence.

3.6 Evidential Graph, Provenance and Admissibility

The correlation workbench is a directed evidential graph, not a picture of guilt. Nodes represent observations, records, persons, infrastructure, organisations, instructions, payments, harms and legal findings; edges state a proposition such as “resolved to”, “authenticated as”, “paid by”, “compiled from”, “tasked by” or “controlled by”. Every edge has an author, source class, time, confidence, method and contrary status. The W3C provenance model supplies a useful general vocabulary for entities, activities and agents, whilst STIX supplies cyber-specific objects; neither, without a MOSAIC profile, distinguishes the legal weight of a forensic observation from that of an intelligence assessment.[16]

The graph should prohibit transitive inference where the rule has not been made express. If an address communicated with a server and that server once hosted malware associated with a group, the system must not infer that the address belongs to the group. If a contractor received payment from a ministry and a subcontractor wrote one library later used in an operation, common financing does not establish knowledge of the target. A proposed path to attribution is a separate inference object which identifies its premises and the rule by which they are joined. Research upon the law and politics of cyber attribution has repeatedly shown that technical, political and legal attribution are related but non-identical acts.[17]

Machine assistance may rank candidate matches, extract entities or detect an unusual sequence, but the unassisted inputs, model version, threshold and validation result remain attached. The United Kingdom’s guidance upon AI and data protection, and NIST’s AI Risk Management Framework, both make governance, documentation, validity and human responsibility relevant where automated analysis affects persons.[18] MOSAIC therefore treats an unexplained embedding similarity as a lead. It cannot become a coercive fact merely because a proprietary model refuses to reveal its path.

For evidential export, the system produces a human-readable schedule and a machine-verifiable package. The schedule states what each item is tendered to prove, who can authenticate it, whether it is original or derived, each transformation, and every known challenge. The package includes source material where law permits, hashes, signatures, trusted times, schema, validation output, software and policy versions, access history and correction chain. International standards upon identification,

[16] World Wide Web Consortium, *PROV-O: The PROV Ontology* (W3C Recommendation, 30 April 2013); OASIS Open, *STIX Version 2.1* (n 8).

[17] Kristen Eichensehr, ‘The Law and Politics of Cyberattack Attribution’ (2020) 67 *UCLA Law Review* 520; Thomas Rid and Ben Buchanan, ‘Attributing Cyber Attacks’ (2015) 38 *Journal of Strategic Studies* 4, 4–37; Jon Lindsay, ‘Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack’ (2015) 1 *Journal of Cybersecurity* 53, 53–67.

[18] Information Commissioner’s Office, ‘Guidance on AI and data protection’ https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ accessed 5 August 2026; National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1, 2023); Government Digital Service, *Artificial Intelligence Playbook for the UK Government* (10 February 2025).

collection, acquisition, preservation, analysis and incident investigation of digital evidence provide useful process disciplines; they do not displace the forum's law of admissibility or disclosure.[19]

English law does not make a computer record true because a computer produced it. The Civil Evidence Act 1995 and Criminal Justice Act 2003 govern hearsay in their respective spheres; the Criminal Procedure and Investigations Act 1996 governs disclosure in criminal proceedings; and familiar authority concerning computer records makes reliability, operation and challenge matters of evidence rather than technological ceremony.[20] A certificate may prove that the national node received a digest at 14.03; a witness, expert or admissible business record must still establish what the originating record means. Where the prosecution cannot disclose material necessary to test a decisive analytic link, fairness may require that reliance be limited or abandoned.

The same distinction matters internationally. A signed preservation receipt is powerful evidence that a State or provider acquired notice and possessed technical capacity to preserve. It is not, without more, proof that the State directed the underlying operation. The software thereby strengthens the omission analysis in Paper 3 without collapsing omission into commission: knowledge, capacity, response and controller-side attribution remain separate propositions.[21]

4. Operating Workflows

Architecture becomes accountable only when one can follow an act from request to conclusion. MOSAIC therefore defines state machines for intake, discovery, preservation, production, correction and manifest access. A message which bypasses its permitted transition is rejected even if sent by an otherwise trusted authority.

4.1 Incident Intake

An incident begins at a reporting organisation, national authority, accredited response company or foreign node. The reporter creates a case object and states, so far as presently known, the affected system, harm, target class, time, urgency and observed indicators. The intake service validates form and identity; it does not require a small water authority in the midst of disruption to make an international-law classification.

The national duty team then separates immediate defence from evidence. Containment advice may be given at once. Original logs are protected from routine deletion. Forensic imaging or volatile capture occurs under the reporter's authority and applicable law. A case officer decides which events should be normalised and whether a wider query is necessary.

The first report may contain error. The system marks it provisional. A report that "China attacked us" is stored as the reporter's assertion, not transformed into the case title. Technical observations are entered separately. This permits a forceful victim account to be preserved without allowing it to govern every later inference.

---

[19] ISO/IEC 27037:2012, *Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*; ISO/IEC 27041:2015, *Guidance on Assuring Suitability and Adequacy of Incident Investigative Methods*; ISO/IEC 27042:2015, *Guidelines for the Analysis and Interpretation of Digital Evidence*; ISO/IEC 27043:2015, *Incident Investigation Principles and Processes*.

[20] Civil Evidence Act 1995; Criminal Justice Act 2003; Criminal Procedure and Investigations Act 1996; *R v Shephard* [1993] AC 380 (HL); *R v Spiby* (1990) 91 Cr App R 186 (CA).

[21] *Corfu Channel (United Kingdom v Albania)* (Merits) [1949] ICJ Rep 4, 22; *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* (Judgment) [1980] ICJ Rep 3, [68]–[74]; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] ICJ Rep 43, [430]; International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001) UN Doc A/56/10.

Where the event meets statutory reporting criteria, MOSAIC may satisfy or route the notice to the designated authority, but it should not create duplicate obligations with inconsistent clocks. A regulated organisation should be able to file once and identify which legal reports have thereby been made. The receipt states precisely which obligations the submission satisfies.

Triage assigns severity upon present and reasonably foreseeable consequences. Immediate loss of money may sit below active danger to life; theft which compromises the solvency of a systemic institution, funds a larger campaign or reveals an innovation capable of replication may be urgent. The classification is revisited as facts emerge. The system does not assume that absence of a corpse at intake makes the aggression trivial.

4.2 Federated Discovery

The case officer selects a set of signals and a time range. The national node transforms them according to the receiving partner’s permitted query mode. Exact values may be hashed under federation-specific keys; structured behaviour may be expressed as a pattern; sensitive intelligence may be represented by a token resolvable only if a match occurs.

The request passes four checks: authority, necessity, proportionality and technical quality. Authority asks whether this role may send this query to these recipients. Necessity asks whether the information is reasonably required for the stated purpose. Proportionality considers scope and protected interests. Quality asks whether the indicator is sufficiently particular and whether time has been normalised.

Recipients execute the query locally. A “no match” answer should distinguish no record from no retained record, unsupported source and inability to search. A positive answer returns a signed assertion containing match type, time band, custodian and contact, but not necessarily the underlying identity. The sending node assembles answers and identifies combinations which merit preservation or human analysis.

Similarity queries require a higher threshold. Before foreign dispatch, an analyst tests the pattern against known benign data where practicable. The recipient may refuse a broad pattern that would search a large part of its population. Rate and breadth controls prevent a State from using cyber cooperation as a general intelligence dragnet.

The workflow target for an authenticated emergency exact query is five minutes to national dispatch and fifteen minutes to automated acknowledgement by an always-on partner. This is a service objective, not a fiction that every legal decision can be made within fifteen minutes. A non-emergency query should receive acknowledgement within four working hours and a substantive routing or refusal decision within one working day.

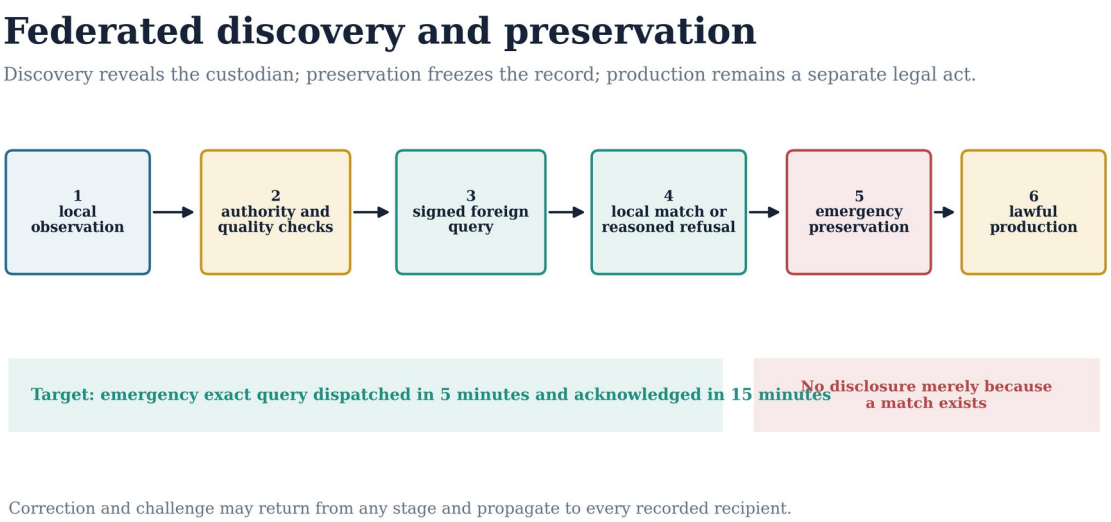

Figure 3. Federated discovery sequence from local observation to signed foreign match, preservation and legally authorised production.

4.3 Emergency Preservation

Preservation freezes identified data; it does not authorise its disclosure. That distinction permits a rapid process with lower immediate intrusion than production. The requesting officer states the evidence sought, custodian if known, time, anticipated offence or protected interest, risk of loss, legal basis and duration. An emergency duty authority approves or refuses.

The national node sends a signed preservation object. The receiving node authenticates the sender, checks whether its law permits execution and routes it to the custodian. The gateway places a hold upon the described records, records the ordinary expiry which would otherwise have applied and returns a signed receipt. If the account or event does not exist, the custodian answers according to a policy which avoids teaching an attacker how to enumerate users.

An initial emergency hold should be short—provisionally seven days where domestic law permits—unless confirmed through the applicable procedure. The precise period will vary by instrument and legal system. The system alerts both authorities before expiry. Extensions identify the judicial, statutory or treaty basis; they are not obtained by resubmitting the same emergency form.

The held data remain subject to access control. Operational analysts need not see them. If the preservation was mistaken, the hold is lifted and ordinary retention resumes; if ordinary expiry passed during the hold, lawful deletion follows unless another basis exists. The receipt remains to show what occurred.

Where danger is immediate and a provider can lawfully take a defensive step—reset an abused credential, isolate a malicious workload or warn a customer—the preservation request may carry a separate recommendation. The provider records whether it acted. Preservation must not become an undeclared shutdown order.

4.4 Production and Legal Process

Discovery identifies a custodian; preservation keeps the evidence alive; production obtains it. The investigator selects the route applicable to the State and data: domestic production order, mutual legal assistance, the Budapest framework, direct cooperation where permitted, a bilateral agreement,

emergency disclosure or voluntary provision. The system generates a request package from the case record but counsel certifies the authority.

The package contains particularised scope, date range, subject identifier, data category, purpose, offences or legal issue, issuing authority, notice restrictions, privilege handling, format, authentication requirement and return channel. It includes preservation receipts so the custodian can locate the held object. Overbroad templates are prohibited.

The custodian may object or seek modification. A conflict-of-law object identifies the competing rule and the authority responsible for resolution. The requesting State can narrow the order, seek government-to-government assistance or contest the objection in the proper forum. MOSAIC records the dispute; it does not decide foreign law by code.

Produced evidence arrives through an encrypted channel into an accredited evidence repository, not the general national-node workbench. Hashes, signatures and provenance are verified. The receiving officer acknowledges integrity and records any failure. Access thereafter follows criminal, regulatory, civil or intelligence rules applicable to the case.

Where a court later excludes evidence, the legal finding is linked to the object and propagated to users who relied upon it. Exclusion for procedural unlawfulness is not necessarily proof that the event did not occur; the system records the reason so a political or defensive assessment does not misread the result.

4.5 Public Attribution and Response Package

A public attribution package is compiled only after technical correlation, intelligence assessment, legal review and policy decision remain separately visible. It includes an executive summary; chronology; affected sectors; observed events; analytic links; identified persons and entities; evidence class; confidence; contrary hypotheses; foreign cooperation; harm; applicable law; and proposed response.

The package contains a disclosure schedule. Some evidence may be published; some shared with allies; some supplied to a court; some protected because its release would expose a source. A minister should be told how much of the conclusion can be defended publicly and what remains classified. “Trust us” may sometimes protect intelligence, but it has a cost which should be explicit.

MOSAIC can calculate neither the existence of an armed attack nor the proportional response. It can display variables relevant to scale and effects: casualties, danger to life, loss of essential services, geographic reach, duration, physical damage, data loss, reversibility, economic consequence, military nexus and reasonably foreseeable maximum harm. Counsel and ministers apply the law.

Where response is taken, the package records measure, authority, objective and review. Sanctions, prosecution, diplomatic protest, service restriction, countermeasure, defensive cyber action and force do not share one legal basis. A common factual record prevents their legal differences from becoming factual inconsistencies.

4.6 Manifest Deposit, Amendment and Opening

A designated controller creates the manifest when an operation is authorised and deposits an encrypted strategic record with the national manifest custodian. Technical components submit signed amendments automatically through the controller gateway. The system checks completeness and alerts the responsible official to missing fields; it does not approve the operation.

Material deviation creates an amendment: expansion of target class, new jurisdiction, subcontractor, autonomous discretion, effect capability or model version. Emergency changes may be recorded

immediately after action within a statutory period, but unexplained retrospective reconstruction is marked. The manifest closes when the operation ends, with a record of retained logs and incidents.

Opening requires a defined trigger. Possible triggers include death or serious physical harm; significant disruption of essential services; credible allegation of unlawful target selection; criminal investigation; judicial order; inspector demand; parliamentary inquiry under secure procedure; or an authenticated request from a harmed State under an applicable agreement. The legislation must define who decides and what part may be disclosed.

Split-key custody can require, for example, one share held by the controller's inspector, one by a senior judicial officer and one by a technical custodian, of which two are required. The arrangement prevents one minister or contractor silently deleting or opening the record. Key rotation, death or incapacity of an officer and institutional reorganisation require tested recovery procedures.

The foreign victim may not receive the full manifest. A court or inspector can verify specified propositions—whether the actor was authorised, whether the target was prohibited, whether the module was registered—without exposing unrelated operations. Privacy-preserving proof cannot answer every contested fact; it can narrow the dispute.

4.7 Correction Workflow

A correction begins when a custodian, analyst, court, subject or partner challenges an object. The originating authority triages urgency: a wrong indicator actively blocking a hospital requires immediate suspension; a disputed historical inference may await review. Recipients are warned that reliance is contested.

An independent analyst examines original evidence, transformation, later facts and the challenge. Outcomes are confirmed, corrected, superseded, withdrawn or unresolved. The decision states reasoning and review route. A correction is signed, linked and pushed to all nodes which acknowledged receipt of the original.

Downstream effect is assessed. If the object supported a preservation notice alone, no further action may be needed. If it materially supported sanctions, prosecution or public attribution, the competent decision owner receives a mandatory review task. The system cannot itself reverse a sanction or judgment.

Performance reporting includes correction time, propagation completion and materially affected decisions. An institution which measures only matches will reward over-claiming; one which measures correction learns whether its speed is safe.

5. Security, Privacy and Abuse

MOSAIC will contain a map of investigations, critical infrastructure, providers, State interests and evidential gaps. Even without raw content it is a target of the first order. Its threat model must include foreign intelligence, organised crime, malicious insiders, compromised providers, corrupt partner nodes, political misuse, supply-chain compromise, model poisoning, denial of service and lawful but excessive use.

The most dangerous failure is not necessarily theft. A subtle attacker may insert false links, suppress matches, alter clocks or learn which indicators cause government concern. Integrity and availability are therefore equal to confidentiality.

5.1 Zero-trust Identity and Access

Every person, service, node and device receives a cryptographic identity bound to role and jurisdiction. Authentication is phishing-resistant; privileged action requires a managed device and, for exceptional functions, a second person. Authorisation is evaluated for each request against case, purpose, data class, recipient and time.

No administrator has unrestricted power over code, keys, evidence and audit. Key custodians, platform administrators, developers, analysts and legal approvers are separated. Privileged sessions are recorded and reviewed. Emergency access is time-limited, conspicuous and subject to next-day independent inspection.

Services use short-lived credentials and mutual authentication. Secrets are held in hardware-backed key management where proportionate. National root keys remain under national control; federation certificates can be revoked rapidly. NIST SP 800-207 supplies the general resource-centred model, whilst the United Kingdom's Cyber Assessment Framework supplies outcome-based security expectations for essential functions.[22]

Policy is code only in the limited sense that repeatable technical rules implement a lawfully approved policy. The human-readable rule, authority, test and deployed version are linked. A silent code change which broadens access is treated as a policy change and requires approval.

5.2 Encryption and Key Management

Data are encrypted in transit and at rest. Particularly sensitive objects may be encrypted end-to-end between competent authorities so intermediate nodes route but cannot read them. Searchable indexes use independent keys and leak only the result authorised by the protocol; their privacy claim is tested rather than assumed.

Keys have purpose, owner, creation, rotation, backup, revocation and destruction records. Split knowledge protects manifest keys and federation roots. Cryptographic agility is designed from the beginning, because a system expected to operate for decades cannot make one algorithm a constitutional commitment.

Metadata deserve protection. The fact that two States are querying a nuclear operator may be as sensitive as the result. Routing should minimise unnecessary visibility; aggregate monitoring must not expose live case relationships. Traffic padding may be justified for the highest classifications, though its cost and latency make universal use wasteful.

5.3 Secure Development and Supply Chain

The programme follows the Government Service Standard and Technology Code of Practice: multidisciplinary delivery, explicit user need, secure service, measurable performance, suitable technology and avoidance of unnecessary supplier lock-in.[23] Secure development includes threat modelling, peer review, automated testing, dependency inventory, signed builds, protected branches, reproducible artefacts where feasible and controlled release.

---

[22] National Cyber Security Centre, 'Cyber Assessment Framework' (n 5); National Institute of Standards and Technology, NIST CSF 2.0 (n 5); National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53 rev 5, 2020, updated 2020).

[23] Government Digital Service, 'Service Standard' https://www.gov.uk/service-manual/service-standard accessed 5 August 2026; Cabinet Office, 'The Technology Code of Practice' https://www.gov.uk/guidance/the-technology-code-of-practice accessed 5 August 2026; HM Government, 'Secure by Design' https://www.security.gov.uk/policy-and-guidance/secure-by-design/ accessed 5 August 2026.

A software bill of materials is maintained for every node release. Dependencies are scanned and patched according to risk. Build and deployment identities are separate; production cannot be altered from a developer laptop. Source and binary provenance are available to participating national assurance teams under appropriate protection.

Open-source components reduce reinvention but do not transfer risk to volunteers. The programme should fund maintenance of critical dependencies it adopts. MISP or OpenCTI can provide adapters and familiar analyst interfaces; neither should be assumed to meet evidential, privacy and sovereignty requirements without assessment.

Suppliers disclose subcontractors, development locations, privileged support arrangements and remote access. National-security review should be principled and repeatable rather than a political label. A supplier excluded for risk receives reasons to the extent possible and a route to challenge consistent with protected intelligence.

5.4 Logging and Protective Monitoring

The NCSC correctly describes logging as the foundation of security monitoring and situational awareness.[24] MOSAIC logs authentication, policy decision, query, match, refusal, export, privilege, administrative change, code deployment and key event. Content is not copied into a log merely for convenience.

Protective monitoring correlates unusual query breadth, protected-category searches, off-hours privileged access, repeated no-match probing, policy overrides, bulk export and failed signature validation. Alerts reach an independent security operations function. The team which investigates analysts should not be managed solely by the operational unit whose productivity it may constrain.

Logs are tamper-evident, segmented and retained according to threat and legal need. A hostile insider should not be able to alter the event and its audit together. Monitoring itself is periodically attacked in exercises, because an untested alarm is a belief.

5.5 Privacy Engineering

A data-protection impact assessment begins before the pilot and is revised with each material function. The UK GDPR principles of purpose limitation, data minimisation, accuracy, storage limitation, security and accountability are represented in fields and controls, not merely the privacy notice.[25]

The system distinguishes personal data necessary to investigate hostile activity from large-scale contextual data which would turn it into general surveillance. Exact matching is preferred where sufficient. Similarity queries are narrower, separately approved and measured for false positives. Protected-category queries require enhanced authority. Bulk historical searches have a published maximum range and an exception process.

Privacy-enhancing techniques may include keyed hashing, private set intersection, secure enclaves, differential privacy for aggregate transparency and selective disclosure credentials. No technique is

[24] National Cyber Security Centre, ‘Introduction to logging for security purposes’ (8 July 2018) https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes accessed 5 August 2026; National Institute of Standards and Technology, *Guide to Computer Security Log Management* (NIST SP 800-92, 2006); Cybersecurity and Infrastructure Security Agency and others, *Best Practices for Event Logging and Threat Detection* (21 August 2024).

[25] Data Protection Act 2018; UK GDPR arts 5 and 25, as amended by the Data (Use and Access) Act 2025; Data (Use and Access) Act 2025; Human Rights Act 1998; Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) art 8; Information Commissioner’s Office, ‘Data protection by design and by default’ https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-by-default/ accessed 5 August 2026.

adopted because its name sounds private. A formal threat model states what the other party learns, what collusion defeats it, how small domains are protected and whether side channels remain.

Data subjects should receive notice when it no longer prejudices the legitimate purpose, except where law authorises continuing secrecy. They should have routes to correction and remedy. National security may justify restrictions; it does not turn inaccurate data into accurate data.

5.6 Insider and Partner Abuse

Insider threat is addressed through vetting, least privilege, separation, monitoring, leave, rotation and a protected reporting route. Behavioural monitoring must itself be proportionate. Suspicion should not arise merely because an employee has family abroad or disagrees with policy.

A partner State may send politically motivated queries concerning dissidents, journalists or commercial competitors. Automated policy blocks prohibited purposes, but wording can be disguised. Protected-category detection, reciprocal audit, random inspection and the right to refuse are necessary. A repeated abuser is moved to a lower trust tier or suspended.

The governance body should publish minimum human-rights criteria for membership and an emergency suspension process. Expulsion may reduce visibility into threats; retaining access may enable abuse. The decision should record both risks rather than assume that cooperation is always benign.

5.7 Resilience and Disaster Recovery

National nodes operate across failure domains with offline recovery material. Provider gateways queue signed requests during network interruption and reject stale emergency commands after expiry. Core service targets are 99.95 per cent monthly availability for national routing and a recovery time objective of four hours for critical federation service, with a recovery point objective measured in minutes for receipts.

A manual emergency channel—pre-registered telephone and signed out-of-band message—exists if the federation is unavailable. It is exercised quarterly. A cyber system which eliminates every non-cyber means of cooperation has confused elegance with resilience.

Backups are encrypted, immutable for defined periods and restoration-tested. Compromise exercises include loss of a national root key, malicious software update, corrupted audit store, cloud-region failure and simultaneous partner suspension. The federation should be capable of isolating one node and continuing amongst the remainder.

Denial-of-service protection includes rate limits, queue priorities, independent communication paths and reserve capacity. An attacker should not be able to flood low-quality notices so that a life-safety preservation expires unseen.

5.8 Threat-led Assurance and Hostile-node Tests

Compliance is a floor and not a rehearsal for the adversary. Before beta, an independent team should be instructed to obtain four outcomes: discover a protected investigation through query metadata; introduce a false association which survives two partner nodes; cause a valid preservation request to expire without a conspicuous alarm; and produce an apparently valid software release outside the approved build path. NIST’s secure-software and supply-chain publications, SLSA provenance

requirements and current government secure-by-design guidance support traceable builds, separation and verification, but the programme must demonstrate these properties in its own deployment.[26]

Software provenance begins before compilation. The authority owns the source repositories, contribution policy, dependency allow-list, build definitions and release keys. Each release carries a software bill of materials in an open format, vulnerability status, source revision, builder identity, test record and approval. The NTIA minimum elements, SPDX and CycloneDX provide interoperable foundations, whilst the in-toto model addresses the more difficult question whether the expected steps occurred in the expected order.[27] A list of libraries is useful; it does not prove that the deployed binary was built from the reviewed source.

Data poisoning is tested independently from code compromise. A hostile provider may return technically valid but systematically misleading matches; an analyst may seed an indicator so that later correlation appears independent; a partner may suppress all negative answers; and a model may be tuned upon a contaminated validation set. The system therefore measures source concentration, circular citation, unusual confidence changes, disagreement amongst custodians and the rate at which one source creates downstream edges. No rule can decide deception automatically. It can expose that nine apparent confirmations originated in the same first allegation.

Privacy tests attempt dictionary and frequency attacks against keyed or set-intersection queries, collusion between a node and custodian, differencing across repeated requests, and inference from response time. Private set intersection can reduce disclosure, but foundational and later protocols show differing computational, trust and leakage assumptions; secure aggregation likewise protects contributions only within its stated adversarial model.[28] The pilot should publish the selected construction, security definition and performance upon representative small domains. A vague statement that identifiers are “hashed” must fail accreditation.

Operational resilience is exercised through loss of the primary cloud region, corruption of the trust registry, revocation of a national root, absence of the senior duty officer, unavailability of a major provider and compromise of the monitoring system itself. Business-continuity and contingency-planning standards require recovery objectives to be tested, whilst the NCSC cloud principles emphasise separation, operational security, audit information and resilience.[29] Restoration succeeds only when the recovered system can prove which messages were accepted before failure and which must be replayed or rejected.

---

[26] National Institute of Standards and Technology, *Secure Software Development Framework (SSDF) Version 1.1* (NIST SP 800-218, 2022); National Institute of Standards and Technology, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (NIST SP 800-161 rev 1, 2022); SLSA, *Supply-chain Levels for Software Artifacts Specification v1.0* (2023); Cybersecurity and Infrastructure Security Agency, *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software* (2023).

[27] National Telecommunications and Information Administration, *The Minimum Elements for a Software Bill of Materials* (12 July 2021); Cybersecurity and Infrastructure Security Agency, *2026 Minimum Elements for a Software Bill of Materials* (July 2026); Linux Foundation, *SPDX Specification 2.3* (2022); OWASP Foundation, *CycloneDX Specification 1.6* (2024); Santiago Torres-Arias and others, ‘in-toto: Providing Farm-to-Table Guarantees for Bits and Bytes’ (28th USENIX Security Symposium 2019) 1393.

[28] Kallista Bonawitz and others, ‘Practical Secure Aggregation for Privacy-Preserving Machine Learning’ (Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security 2017) 1175, 1175–91; Kissner and Song (n 7); Freedman, Nissim and Pinkas (n 7); Pinkas, Schneider and Zohner (n 7).

[29] ISO 22301:2019, *Security and Resilience—Business Continuity Management Systems—Requirements*, as amended by ISO 22301:2019/Amd 1:2024; National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information Systems* (NIST SP 800-34 rev 1, 2010); National Cyber Security Centre, ‘The cloud security principles’ https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles accessed 5 August 2026.

Assurance remains independent through procurement. A supplier may test its work, but cannot be the sole judge of its own cryptography, evidential export or exit plan. At least annually, a security laboratory, a privacy team, a forensic practitioner and counsel should each receive a defined challenge. Findings are tracked to closure; residual risk is accepted by a named Crown official; and the public report states the number and severity of unresolved findings in bands where details would be dangerous. A “red team passed” badge, unconnected to scope and date, is advertising rather than evidence.

6. Legal and Institutional Integration in the United Kingdom

The United Kingdom should not construct MOSAIC upon administrative enthusiasm alone. Its compulsory functions require statute; voluntary exchange requires clear public-law authority, data-protection basis and agreements; intelligence use requires the existing statutory regimes applicable to the body concerned.[30] Paper 5 supplies the wider legislative model. This section specifies the clauses required by the software.

6.1 Statutory Functions

The statute should designate a United Kingdom MOSAIC Authority and confer functions to operate the national node; accredit gateways; receive and route incident notices; issue emergency preservation notices within defined criteria; maintain the trust registry; coordinate lawful international requests; operate the manifest custodian; publish technical standards; and report.

It should not merge investigative powers. A request for data must identify the independent enactment, warrant, order, consent or agreement authorising it. The MOSAIC Act may create a narrowly drawn preservation power because speed is its purpose, but production and interception should remain under the regimes drafted for those intrusions unless Parliament expressly amends them.

The present statutory baseline must be stated accurately. The Network and Information Systems Regulations 2018 remain in force. As at 5 August 2026, the Cyber Security and Resilience Bill had completed Commons second reading and committee stage but had not become an Act; its proposed expansion of regulated entities and power of direction are therefore relevant institutional design, not an existing source of MOSAIC authority.[31] The software should be capable of mapping later reporting duties, but neither a business case nor an API may anticipate Parliament by treating a Bill as law.

Mandatory participation should begin with central government, designated operators of essential services, relevant digital service providers, accredited PMSCs conducting high-risk cyber operations for the Crown and providers under substantial government cyber contracts. Extension to further classes should occur by affirmative regulations following consultation, necessity assessment and technical support.

Small organisations require funded gateways or a simple reporting portal. A duty which assumes a permanent security operations centre will punish precisely the vulnerable bodies whose evidence the system needs. The NCSC’s history of supporting attainable logging for smaller organisations supplies the right practical instinct: establish a reliable flight recorder, then improve it.[32]

---

[30] Investigatory Powers Act 2016, as amended by the Investigatory Powers (Amendment) Act 2024; National Security Act 2023; Computer Misuse Act 1990.

[31] Network and Information Systems Regulations 2018, SI 2018/506; Department for Science, Innovation and Technology, ‘Cyber Security and Resilience Bill’ https://www.gov.uk/government/collections/cyber-security-and-resilience-bill accessed 5 August 2026; Department for Science, Innovation and Technology, ‘Summary of the Cyber Security and Resilience Bill’ (30 June 2026) https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill accessed 5 August 2026.

6.2 Preservation Power

An emergency preservation notice should require reasonable grounds to believe that specified data relate to a serious cyber incident or imminent serious harm and are at material risk of alteration or deletion. It identifies data, custodian, period, approving officer, purpose and route to challenge. It prohibits destruction of the preserved copy but does not compel disclosure.

Because preservation interferes with data rights and may impose cost, the notice should be necessary and proportionate. Initial duration should be short and extension subject to judicial or designated independent approval. Providers receive reimbursement for exceptional reasonable cost and protection for good-faith compliance with a facially valid notice, without immunity for negligent disclosure.

Intentional destruction after service is an offence; accidental failure is addressed through civil penalty according to fault and impact. The statute should avoid criminalising a provider which could not technically identify the record or suffered an independent outage. False certification by a requesting official is likewise sanctionable.

Foreign notices are executed only through an applicable legal basis. A protocol signature proves origin; it does not create British authority. The United Kingdom may enter agreements recognising equivalent partners, subject to human-rights and oversight safeguards.

6.3 Incident Reporting and Secrecy

Reporting thresholds should identify serious incidents by actual or reasonably foreseeable effect upon essential services, national security, economic stability, democratic institutions, life, physical safety, substantial data integrity or systemic financial loss. “Maximum possible harm” cannot mean any imaginable catastrophe; the correct measure is the maximum reasonably credible and foreseeable consequence supported by capability, access and target.

Initial notice should be rapid and limited—within hours for the most serious events—followed by staged reports as facts become available. A regulated body should not delay defence in order to compose a perfect attribution. Deliberately false or reckless reports may be penalised; good-faith preliminary error should not.

Confidentiality protects commercial, personal, security and intelligence material. Unauthorised disclosure is sanctioned. Yet secrecy cannot be absolute: evidence may be disclosed for investigation, court, regulator, parliamentary oversight, warning and international cooperation under defined controls.

6.4 Controller and PMSC Duties

A government department commissioning a cyber operation, and a PMSC accepting it, should maintain an attribution manifest, identifiable command, subcontractor register, software and model inventory, incident reporting, stop mechanism and audit access. Contracting cannot reduce the Crown’s legal duties. Subcontracting must not dissolve operational control into invoices.

The prime contractor remains responsible for ensuring that lower tiers produce required technical records. A coder who lawfully writes an isolated library without knowledge of hostile use is not thereby made a combatant or criminal. The manifest identifies who knew the objective, who could alter target selection and who controlled effect.

[32] National Cyber Security Centre, ‘Logging Made Easy’ (updated 18 September 2025) https://www.ncsc.gov.uk/information/logging-made-easy accessed 5 August 2026; National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response* (NIST SP 800-86, 2006); ISO/IEC 27037:2012.

Where autonomous systems select targets, techniques, timing or jurisdictional route, the controller records the permitted decision space, tests, constraints and human authority. “The AI decided” is not a legal person and not an answer to who deployed it with that discretion.

6.5 Courts, Disclosure and Evidential Weight

MOSAIC records should not be made self-proving by legislative declaration. A signature may establish authenticity of a message; the truth and weight of its contents remain open. Domestic evidential rules determine admissibility, expert opinion, hearsay, public-interest immunity, disclosure and fairness.

The statute may permit certificates concerning routine technical matters—node identity, receipt time, hash verification and system operation—subject to challenge. A defendant must be able to contest a material analytic link. If protected intelligence is indispensable and cannot be fairly tested, the court applies the existing procedures and may exclude or limit reliance.

Courts should be able to order correction of the national node following a finding. A judicial determination is entered as such, not merely another analyst opinion. The system records whether the finding was final, appealed or limited to procedure.

6.6 International Agreements

A MOSAIC agreement should define competent authorities, permitted purposes, data classes, preservation, production routes, human-rights safeguards, onward transfer, retention, security, audit, breach notification, costs, refusal, suspension, remedy and dispute resolution. Technical annexes define protocol and conformance; they can be updated more readily than the treaty without changing legal power.

The Second Additional Protocol to the Budapest Convention and Regulation (EU) 2023/1543 demonstrate that faster electronic-evidence cooperation can be built with conditions and safeguards.[33] MOSAIC should interoperate with, not duplicate, those routes. Where a partner is outside them, a bilateral or limited arrangement may support defensive matching and preservation pending ordinary assistance.

The United Kingdom should offer reference gateway software and onboarding grants to lower-capacity partners. Otherwise the federation will consist only of States which already possess visibility, leaving the jurisdictions most attractive for outsourced fragments outside it. Capacity support is not charity; it closes a route by which hostile controllers externalise cost.

No agreement should require a State to accept another’s public attribution or legal characterisation. Partners agree to authenticate, preserve, answer or give a reason. Political judgement remains sovereign.

6.7 Rights, Retention and Constitutional Control

The fact that MOSAIC is federated does not remove its interference with private life; it changes where the interference occurs and which actor can see it. The European Court of Human Rights’ bulk-surveillance cases require end-to-end safeguards, including assessment at each stage, independent authorisation appropriate to the measure, supervision and ex post review. The Court of Justice’s data-retention authorities likewise reject general and indiscriminate retention as an ordinary answer to

[33] Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime* (CETS No 224, 2022); Cybercrime Convention Committee, *24/7 Points of Contact Network of the Budapest Convention on Cybercrime: Assessment Report* (T-CY(2020)2, 2020); Council of Europe, *Guide to the Implementation of the Second Additional Protocol to the Convention on Cybercrime in Domestic Law* (2025); US Department of Justice, *The Purpose and Impact of the CLOUD Act* (April 2019).

serious crime, although they recognise carefully delimited measures under stated conditions.[34] MOSAIC's case-bound query and local custody are designed in answer to that jurisprudence, but they will comply only if exceptions remain exceptional in operation.

Retention is therefore set by object and purpose. A routing receipt may be needed long enough to audit cooperation; an unsuccessful query against a protected person may require shorter operational retention but a sealed oversight record; produced criminal evidence follows the case regime; a manifest follows the operation and statutory limitation; and aggregate service measures cease to identify the subject. Legal hold suspends ordinary deletion only for the material and proceeding identified. The Public Records Act, Freedom of Information Act, Official Secrets Act and data-protection legislation address different questions and must not be compressed into a single "government retention" label.[35]

The statute should require a code of practice approved by Parliament. It should state request classes, protected categories, urgency, permitted data, authorisation, review, retention, notice, correction, security, partner suspension and transparency. Material changes to the protocol which alter who may query what are changes to the exercise of public power, even if expressed as software configuration. They should receive the same approval and publication required for the corresponding rule, subject only to the redaction necessary to protect a technical vulnerability.

Independent offices should not be given overlapping titles and uncertain responsibility. The Information Commissioner supervises data protection; the Investigatory Powers Commissioner supervises powers within that statutory jurisdiction; courts determine live disputes; and Parliament scrutinises policy and expenditure. The MOSAIC commissioner, if a new office is justified, should oversee the preservation power, federation use, manifests and correction which fall between those regimes, and should possess a duty to refer matters which belong elsewhere. Multiplying commissioners without allocating questions produces the appearance of oversight and the practice of referral.

Extraterritorial caution remains essential. In *KBR Inc v Director of the Serious Fraud Office* the Supreme Court reaffirmed the presumption that Parliament does not ordinarily intend an investigatory power to compel a foreign company abroad, a presumption rooted in international law and comity. The litigation surrounding data held by Microsoft abroad, and the later CLOUD Act response, demonstrate how location, control and statutory language can outrun traditional process.[36] MOSAIC's foreign signature proves the request's origin and permits speed; compulsion must still come from express law and an applicable territorial or agreed route.

---

[34] *Big Brother Watch and others v United Kingdom* (2022) 74 EHRR 17; *Centrum för rättvisa v Sweden* [GC] App no 35252/08 (25 May 2021); *Roman Zakharov v Russia* [GC] App no 47143/06 (4 December 2015); *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; Kärntner Landesregierung* (Joined Cases C-293/12 and C-594/12) EU:C:2014:238; *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson and others* (Joined Cases C-203/15 and C-698/15) EU:C:2016:970; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* (Case C-623/17) EU:C:2020:790; *La Quadrature du Net and others v Premier ministre and others* (Joined Cases C-511/18, C-512/18 and C-520/18) EU:C:2020:791; *Prokuratuur* (Case C-746/18) EU:C:2021:152; *SpaceNet AG and Telekom Deutschland GmbH* (Joined Cases C-793/19 and C-794/19) EU:C:2022:702.

[35] Public Records Act 1958; Freedom of Information Act 2000; Official Secrets Act 1989; Data Protection Act 2018.

[36] *R (KBR Inc) v Director of the Serious Fraud Office* [2021] UKSC 2, [2022] AC 519, [21]–[27]; *Microsoft Corporation v United States* 829 F 3d 197 (2d Cir 2016), vacated as moot 584 US 236 (2018); US Department of Justice, *The Purpose and Impact of the CLOUD Act* (April 2019); Crime (Overseas Production Orders) Act 2019.

Nor may the evidential service acquire, by administrative drift, a power to decide war. A package which records scale, effects and reasonably foreseeable harm may support a government's legal assessment, but the Charter rules upon force and self-defence remain independent; the United Kingdom's published cyber position recognises that cyber operations may in grave cases engage those rules.[37] MOSAIC can shorten the time before facts disappear. It cannot lower the legal threshold because the facts arrived quickly.

7. Costed Options

A cost which appears precise without assumptions is ornament. The following figures are planning estimates in 2026 pounds, excluding VAT, financing, ordinary participant logging and the salaries of investigators who would exist without MOSAIC. They include programme labour at fully loaded cost, platform infrastructure, specialist assurance, partner enablement, equipment and contingency. They do not purport to replace a Green Book business case or competitive market testing.

HM Treasury requires public appraisals to address systematic optimism and to adjust cost, benefit and duration where the evidence supports it.[38] MOSAIC is predominantly a software development and integration programme, with difficult international and legal dependencies. The estimates therefore apply an approximately thirty per cent programme contingency after component-level allowances. This is materially below the historic upper bound cited in the Treasury's generic equipment and development guidance and assumes strong modular delivery, early testing and the ability to stop after the pilot. A full business case should revise it with reference-class data from comparable secure government systems.

Three options are costed:

- **Constrained federation**: four national partners, about 250 reporting organisations, twenty million normalised events indexed each month, business-hours ordinary service and on-call emergency preservation.
- **Core federation**: twelve national partners, about 2,000 reporting organisations, 250 million normalised events each month, continuous national-node operations and funded onboarding.
- **Extended federation**: thirty national partners, about 10,000 reporting organisations, two billion normalised events each month, multiple security domains, greater language and legal support and higher resilience.

The event volume is an index and query assumption, not a proposal to centralise that number of raw logs. Local gateways perform normalisation and matching. Federation cost grows principally with partners, assurance, support, query rate and legal complexity rather than bytes alone.

7.1 Twelve-month Pilot

The pilot should prove one complete chain with the United Kingdom and three willing partners, not exhibit every future function. It would include a United Kingdom national node; reference and hosted gateways; exact and privacy-preserving matching; preservation receipts; one manifest proof of concept;

[37] Charter of the United Nations arts 2(4) and 51; Foreign, Commonwealth & Development Office, *Application of International Law to States' Conduct in Cyberspace: UK Statement* (3 June 2021); Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) rr 69 and 71; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14; *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* (Judgment) [2005] ICJ Rep 168.

[38] HM Treasury, *The Green Book: Central Government Guidance on Appraisal and Evaluation* (2026) https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2026 accessed 5 August 2026; HM Treasury, 'Green Book supplementary guidance: optimism bias' (21 April 2013) https://www.gov.uk/government/publications/green-book-supplementary-guidance-optimism-bias accessed 5 August 2026; Government Project Delivery, *The Teal Book* (version 3.0, 2026); Government Project Delivery, *Government Functional Standard GovS 002: Project Delivery* (version 2.1, 2025).

a simulated production package; correction propagation; zero-trust identity; audit; independent security testing; and exercises involving an operator of essential services, cloud provider, registrar and law-enforcement body.

The cost is estimated as follows:

Table 1. MOSAIC twelve-month pilot cost in 2026 pounds.

Pilot component	Assumption	Cost (£m)
Product, engineering and user research	18 average FTE at £135,000 loaded	2.43
Security engineering and operations	7 average FTE at £150,000 loaded	1.05
Legal, evidence, privacy and international policy	7 average FTE at £140,000 loaded	0.98
Programme, commercial and partner delivery	6 average FTE at £125,000 loaded	0.75
Cloud, development environments and secure tooling	multi-environment pilot	0.70
Hardware security, test gateways and protected connectivity	four national nodes and laboratory	0.65
Independent penetration, architecture, privacy and evidential assurance	staged external reviews	0.75
Partner grants, training, exercises and translation	three partners and UK participants	0.85
Subtotal		8.16
Contingency and optimism allowance	30% for first-of-kind pilot	2.45
Pilot total	rounded	**10.61**

The loaded FTE rate includes salary, pension, National Insurance, accommodation, equipment and ordinary overhead; it is not the employee’s salary. Security-cleared engineering and specialist legal evidence roles are deliberately costed above a general public-sector average. Procurement should test these assumptions and disclose material change.

At the end of twelve months the programme should not automatically proceed. Entry to the core build requires: successful exchange amongst all four nodes; preservation receipt within the tested service target; complete audit reconstruction; correction propagation; no unresolved critical security finding; a lawful-basis and human-rights review; participant evidence that the workflow reduces time; and an approved full business case. A pilot which proves that the legal diversity cannot be reconciled cheaply has delivered value by preventing a larger failure.

7.2 Core Three-year Programme

The core option is the recommended minimum capable of changing the attribution problem. Four partners may prove a protocol; twelve begin to cover the mixed cloud, registrar, payment and contractor routes encountered in practice. The programme assumes an average of sixty-seven directly funded FTE over three years, rising during build and reducing in some engineering roles as operations stabilise.

Table 2. MOSAIC core three-year programme cost in 2026 pounds.

Core component	Three-year assumption	Cost (£m)
Product and engineering	average 27 FTE at £140,000	11.34
Security, reliability and continuous monitoring	average 15 FTE at £150,000	6.75
Legal, evidence, privacy and oversight support	average 11 FTE at £140,000	4.62
Programme, commercial and service management	average 8 FTE at £125,000	3.00
International onboarding, training and user support	average 6 FTE at £120,000	2.16
Cloud, storage, observability and protected development	scaled environments and reserve capacity	4.80
Hardware security modules, node kits and protected networks	UK core and partner enablement	3.60
Independent assurance and red-team programme	annual technical, legal and privacy examination	2.40
Partner implementation grants	eleven partner packages at differentiated rates	5.50
Exercises, documentation, translation and adoption	sector and international exercises	1.80
Contingency for transition and data migration	component allowance	1.03
Subtotal		47.00
Programme contingency and optimism allowance	30.2% of subtotal	14.20
Core three-year total	rounded	**61.20**

The percentage is stated because a rounded “twenty per cent” would not produce the number. The larger allowance reflects international onboarding, assurance findings and first-of-kind integration, whilst component estimates already contain ordinary operational overhead. If better comparable data support a lower figure at full business case, the released amount should remain gated rather than treated as available scope.

The steady-state United Kingdom operating cost after year three is estimated at £11–14 million annually for approximately fifty-five core staff, infrastructure, assurance, support and periodic exercises. Partner States fund their ordinary node operations after tapered grants. Material expansion in retained central data, classified domains or compulsory small-provider support would increase that sum.

7.3 Constrained and Extended Options

The constrained three-year option is estimated at £29.6 million: £22.8 million component cost and £6.8 million contingency. It uses approximately thirty-four average FTE, four partners, limited hosted gateways and lower availability for non-emergency work. It could improve national preservation and bilateral cooperation, but it leaves the system vulnerable to route-around. A controller can prefer jurisdictions outside four partners. The option is useful if international agreement proves slower than engineering; it is not the full answer claimed by Paper 3.

The extended option is estimated at £125.6 million: £96.6 million component cost and £29 million contingency. It supports thirty States, many more small entities, several protected security domains, twenty-four-hour multilingual legal support, higher query rate and grants for lower-capacity partners. It assumes approximately 145 average funded FTE across the United Kingdom programme and common services, not the staff of all national nodes. It should not be selected at outset. It is a scale path triggered only after core performance and independent evaluation.

Table 3. Comparison of constrained, core and extended MOSAIC options.

Measure	Constrained	Core	Extended
National partners	4	12	30
Reporting organisations	c 250	c 2,000	c 10,000
Monthly locally indexed events	20m	250m	2bn
Average funded FTE	34	67	145
Three-year estimate	£29.6m	£61.2m	£125.6m
Ordinary availability	business hours plus emergency on-call	continuous national routing	continuous multi-domain
Principal weakness	easily routed around	incomplete global reach	cost, governance and attack surface

These are not alternative prices for the same benefit. The constrained system answers “can four partners act quickly?”; the core system answers “can a meaningful federation correlate a distributed campaign?”; the extended system addresses wider route-around and capacity. The economic case must value the additional coverage rather than choose the lowest number because it is lower.

Figure 4. Three-year planning estimates for constrained, core and extended deployment, in 2026 pounds.

7.4 Benefits and the Cost of Absence

Benefits should not be inflated by assigning MOSAIC the whole value of every incident it touches. The service may shorten detection, preserve evidence, prevent duplicated requests and support faster containment. It does not create the underlying security control or guarantee that evidence leads to recovery.

Measurable direct benefits include analyst hours saved; requests avoided through discovery; records preserved which would otherwise expire; reduction in time to identify a custodian; fewer duplicate reports; faster warning to similarly exposed organisations; reduction in incorrect associations through correction; and reusable gateway compliance. These can be measured during pilot.

Avoided-loss modelling should use scenarios and ranges: a destructive attack upon a hospital group; temporary water disruption; theft from a financial institution; election-system compromise; and a contractor campaign against several sectors. For each, analysts should estimate the part of consequence plausibly reduced by earlier correlation, not the entire gross loss. Sensitivity should show what frequency and reduction make each option worthwhile.

There is also option value. A system capable of confirming within an hour that apparently isolated fragments form a critical-infrastructure campaign permits action before certainty becomes retrospective. The value is largest where harm is nonlinear—winter energy interruption, contaminated control process, loss of unique data or replicated autonomous intrusion. That value is difficult to monetise but not unreal.

Opportunity cost remains. £61.2 million could fund baseline security, hospital resilience, police, diplomacy or provider grants. The core business case should compare MOSAIC with improving domestic logging alone, expanding existing international teams, subsidising provider retention and relying on current treaty processes. Federation is justified only where the correlation and preservation gap cannot be solved by those measures separately.

7.5 Procurement and Commercial Structure

The United Kingdom should procure outcomes and components rather than one indefinite prime contract. A Crown-owned protocol, schema, reference implementation and export format preserve sovereignty. Competing suppliers may provide hosting, connectors, user interface, testing and support. The Authority retains architecture, keys, accreditation and the ability to transition.

The programme should publish a modular procurement map:

1. core federation and policy engine;
2. gateway and connector framework;
3. cryptographic and key services;
4. correlation workbench;
5. evidence export and manifest custody;
6. security operations and assurance;
7. partner onboarding and training.

No supplier should both develop a security-critical component and provide its only independent assurance. Commercial terms require vulnerability disclosure, incident notification, escrow or transition of essential material, supply-chain transparency, data-return testing and assistance upon exit.

Open-source release is appropriate for schemas, test harnesses, gateway reference code and non-sensitive interoperability components. Sensitive detection and deployment details may remain

protected. Public code is not automatically secure; private code is not automatically sovereign. Reproducible testing and the right to inspect matter more than the label.

Payment should follow gated deliverables: conformance, performance, security, evidential export and exercised recovery. A dashboard count of “features delivered” invites the easiest features. The contract should reward working cross-organisational journeys.

7.6 Cost Method, Sensitivity and Affordability Gates

The estimates are a reference-class planning model and not a quotation. They multiply fully loaded role-years, infrastructure allowances, partner grants and fixed assurance packages; then they add a separately visible contingency. The Green Book requires options to be compared by social costs, benefits and risks rather than by the cash price of the preferred scheme, whilst supplementary optimism-bias guidance requires explicit uplifts where robust project-specific evidence is absent. The 2026 Teal Book and Project Delivery Functional Standard add the practical requirements of an evidence-based baseline, accountable ownership, change control and benefits management.[39]

Three variables dominate. If average funded staffing rises by twenty per cent without scope reduction, the core component estimate increases by approximately £5.2 million before contingency. If twelve partners each require £500,000 more integration support, the component estimate rises by £6 million. If security classification requires a second protected environment with separate operations, a further planning allowance of £7–10 million over three years is reasonable pending design. Conversely, reuse of proven gateways and lower partner grants may reduce cost; the programme must not spend a released contingency merely because the risk did not occur.

Table 4. Illustrative sensitivity of the core three-year estimate.

Scenario	Component change before programme contingency	Indicative total effect	Required decision
Base core option	none	£61.2m	proceed only after pilot gate
Staff cost or effort +20%	+£5.2m	c £68.0m	rebaseline roles and benefits
Partner integration +£0.5m each	+£6.0m	c £69.0m	test coverage value partner by partner
Separate protected environment	+£7–10m	c £70–74m	approve only for identified classified journeys
Reuse reduces gateway and platform cost by £4m	−£4.0m	c £56.0m	retain unused contingency behind gate

The indicative totals apply the same approximate contingency relationship and are rounded; they are not arithmetic promises. At full business case, each should be replaced by supplier testing, departmental pay and overhead data, cloud consumption models, partner discovery and quantified risk. The AQuA

[39] HM Treasury, *The Green Book* (n 38); HM Treasury, ‘Optimism bias’ (n 38); Government Project Delivery, *The Teal Book* (n 38); Government Project Delivery, *Government Functional Standard GovS 002* (n 38).

Book requires analytical assumptions, quality assurance and proportionate independent challenge; the Orange Book requires risk to remain connected to governance and decision.[40]

Affordability gates bind scope to benefit. Before alpha, the authority approves no more than the foundation and synthetic exercise. Before beta, it must demonstrate four interoperable nodes, a tested exit route and an updated whole-life cost. Before core scale, it must show that preservation time, evidence survival and analyst effort improved against the counterfactual; technical success without operational benefit is not enough. Before the extended option, it must show that route-around through absent jurisdictions is a measured cause of failure and that the proposed new partners cover it.

Supplier concentration is itself a cost risk. The Procurement Act 2023 and the Sourcing Playbook favour transparent, effective procurement and deliberate make-or-buy analysis; the National Audit Office has warned that government's dependence upon technology suppliers, subscription services and legacy estates requires stronger commercial intelligence and exit planning.[41] MOSAIC should therefore cost transition from its first business case: data and configuration export, replacement of hosted gateways, transfer of keys, documentation, staff knowledge and thirty-six months of security history. A low bid which makes those assets inaccessible is deferred expenditure disguised as economy.

Evaluation also has a cost and must be funded. The Magenta Book distinguishes process, impact and value-for-money questions; each is necessary here.[42] Process asks whether requests move and rights controls operate. Impact asks whether material which would otherwise disappear is preserved and whether decisions improve. Value for money asks whether those gains exceed the opportunity cost of domestic logging grants, investigators or provider retention. No honest design can guarantee the answer before pilot, which is why the stop decision is an achievement rather than an embarrassment.

8. Delivery and Integration

MOSAIC should proceed in four gates over thirty-six months. The times are demanding but achievable because the first objective is not global unanimity; it is a complete narrow service with willing partners.

8.1 Gate One: Foundation, Months 0–3

The sponsoring department appoints a senior responsible owner, product director, chief architect, senior legal owner, security officer, evidence lead and independent assurance chair. Parliament receives the proposed power and safeguard outline. The team maps users and existing systems at NCSC, NCA, sector bodies, providers and partners.

The programme publishes problem statement, threat model, draft schema, privacy plan, commercial strategy and pilot metrics. It selects three partners according to legal compatibility, operational relevance and technical willingness, not political ceremony. At least one should be a smaller-capacity jurisdiction to test whether the design merely assumes wealth.

Existing threat-intelligence platforms, reporting portals, case-management systems and evidence stores are inventoried. Interfaces are defined; wholesale replacement is prohibited unless separately justified. The programme chooses pilot incident types and constructs synthetic datasets which reproduce legal and technical complications without exposing live victims.

---

[40] HM Treasury, *The AQuA Book: Guidance on Producing Quality Analysis for Government* (2025); HM Treasury, *The Orange Book: Management of Risk—Principles and Concepts* (updated 2026).

[41] Procurement Act 2023; Cabinet Office and Government Commercial Function, *The Sourcing Playbook* (updated 15 June 2026); National Audit Office, *Government's Approach to Technology Suppliers: Addressing the Challenges* (16 January 2025).

[42] HM Treasury, *The Magenta Book: Central Government Guidance on Evaluation* (updated 15 May 2026).

Exit requires approved alpha architecture, statutory path, data-protection impact assessment, partner memoranda, cost baseline and red-team plan.

8.2 Gate Two: Alpha and Closed Exercise, Months 3–6

The team builds national-node minimum service, two gateway types, trust registry, exact query, preservation object, receipt store, correction and audit. It implements the STIX/TAXII profiles and MOSAIC extensions. Human workflows are tested with duty officers, provider counsel, investigators and oversight staff.

A closed exercise begins with a synthetic attack divided across the four jurisdictions. One fragment expires rapidly, one query concerns a protected category, one provider raises conflicting law, one node is compromised and one initial indicator is wrong. Success requires not merely finding the campaign but preserving rights and correcting the error.

Independent testers examine protocol, code, keys, privacy, accessibility, evidential continuity and insider controls. Critical findings block progression. The cost and delivery forecast is rebaselined.

8.3 Gate Three: Beta Pilot, Months 6–12

Accredited public and commercial participants connect real security logs under limited scope. The service handles selected live incidents with human supervision. Emergency preservation is used only where legislation or existing authority permits. No autonomous coercive action is introduced as a pilot shortcut.

Performance, match quality, false association, preservation time, provider burden, refusal and user comprehension are measured. Oversight receives live audit access. A public interim report states what can be disclosed, including cost and changes from plan.

At month twelve an independent panel decides whether to stop, extend the pilot or enter core scale. Its report addresses security, legality, operational benefit, partner trust and cost. Ministerial desire to announce a federation is not an acceptance criterion.

8.4 Gate Four: Core Scale, Months 12–36

The programme adds partners in cohorts of two or three. Each completes legal mapping, node conformance, security assessment, exercise and oversight agreement before live access. Reporting organisations are onboarded by sector, beginning with government and critical services, then high-risk providers and designated contractors.

Manifest custody progresses separately because its classification and constitutional risks differ from defensive correlation. A domestic PMSC and government proof of concept precedes foreign interoperability. The evidential export service is tested in mock and, when available, actual proceedings.

Operations, engineering and policy teams separate gradually. A service which remains permanently in project mode tends to evade operational accountability; one which freezes at launch fails against changing threats. Product governance must permit controlled iteration.

At month thirty-six Parliament receives the independent evaluation, revised operating cost and recommendation upon extension. Sunset or renewal should apply to novel preservation and manifest powers even if the technical service continues for voluntary defensive exchange.

8.5 Integration Rather than Replacement

NCSC already receives and analyses cyber reports; NCA and police operate investigative systems; providers possess abuse and legal-response portals; regulators maintain incident regimes; international channels exchange threat intelligence and evidence. MOSAIC should supply common identity, schema, receipt and federation rather than demand that every body abandon its case system.

Adapters map existing incident identifiers and preserve a link to the system of record. The national node stores only what the cross-organisational journey needs. A police case-management system remains responsible for criminal files; an intelligence system for classified holdings; a regulator for enforcement. Duplication is measured and reduced.

Provider integration offers an API, portal and managed gateway. Large providers may automate; small organisations file through a supported portal or accredited service. The interface reports legal route and status in plain language. It should never require a local council to understand TAXII in order to preserve a log.

The federation should reuse existing trusted relationships where lawful: national computer-security incident response teams, the Budapest 24/7 Network, law-enforcement channels and bilateral cyber dialogues. A new protocol need not create a new diplomat for every message.

8.6 Legacy, Cloud and Operational-technology Integration

The easiest organisation to connect will be the one which already retains structured security events, has a modern identity service and can expose a controlled API. The most important evidence may instead sit in a local authority, hospital supplier, water operator or ageing industrial device whose clock, storage and authentication cannot be replaced during an incident. The gateway design must therefore support three modes: native API for capable providers; managed collector for ordinary legacy systems; and an offline or human-assisted preservation package for isolated operational technology.

No gateway should be placed in the safety-control path merely to improve attribution. In operational technology, availability and deterministic behaviour may outweigh the convenience of real-time export. The collector should ordinarily receive a one-way or carefully brokered copy, maintain its own trusted receipt time, and queue signed summaries if the external route is unavailable. NCSC guidance upon cloud-hosted SCADA and joint guidance adapting zero-trust principles to operational technology emphasise legacy constraints, safety, observability and architecture suited to the environment rather than the indiscriminate transplantation of enterprise controls.[43]

Cloud integration begins at the control plane. Account creation, identity assumption, policy change, workload launch, image digest, network attachment and region are often more probative than the short-lived workload's filesystem. NIST's cloud forensic reference architecture and earlier study of cloud forensic challenges identify the distribution of responsibilities, ephemerality, multi-tenancy and dependence upon provider interfaces.[44] MOSAIC adapters should preserve the provider's native event and map it to the common schema, never discard an inconvenient field merely because the national model does not yet understand it.

Interoperability is versioned at the boundary. STIX and TAXII profiles, MISP and OpenCTI adapters, evidence exports and preservation objects receive conformance suites containing valid, invalid and

[43] National Cyber Security Centre, 'Cloud-hosted SCADA' https://www.ncsc.gov.uk/collection/operational-technology/cloud-hosted-scada accessed 5 August 2026; Cybersecurity and Infrastructure Security Agency and others, *Adapting Zero Trust Principles to Operational Technology* (29 April 2026).

[44] National Institute of Standards and Technology, *NIST Cloud Computing Forensic Reference Architecture* (NIST SP 800-201, 2024); National Institute of Standards and Technology, *NIST Cloud Computing Forensic Science Challenges* (NISTIR 8006, 2014); Fang Liu and others, *NIST Cloud Computing Reference Architecture* (NIST SP 500-292, 2011).

adversarial examples. A provider may implement the protocol without buying the central workbench. The Cloud Security Alliance control matrix and NIST cloud reference architecture may assist assurance mapping, but accreditation attaches to the deployed gateway, its configuration and legal role rather than to a generic product.[45]

Migration occurs by incident journey, not database. The first release takes one report from a selected organisation through exact discovery, preservation, lawful production, correction and oversight. Only after that path works does the programme add similarity, further sectors or manifests. The Government Service Standard and Technology Code of Practice support iterative, user-centred, measurable services; the National Audit Office's accounts of digital transformation show the cost of layering new interfaces upon unresolved legacy, data and ownership problems.[46] A programme which connects two thousand organisations but cannot complete one evidential journey has counted installation rather than capability.

9. Testing, Evaluation and Public Measures

A serious system tests the proposition that it is safe to use, not merely that it runs. MOSAIC requires functional, interoperability, security, privacy, evidential, legal, resilience and human-factors testing.

Conformance suites should be public and versioned. A node must demonstrate signature validation, policy enforcement, refusal, expiry, correction and compromise handling. Passing message syntax alone is inadequate.

Security testing includes source review, dependency analysis, penetration, red-team operations, insider scenarios and recovery. Privacy testing measures information leaked by queries, small-domain reversal, linkage and protected-category controls. Evidential testing asks an independent lawyer and forensic expert to reconstruct collection and transformation without assistance from the original developer.

Legal tabletop exercises place counsel from differing States around the same request. They identify where a field cannot cure a conflict and where an agreement is needed. Human-factors testing observes whether a duty officer under pressure understands preservation versus production, confidence and expiry.

The principal public measures are:

- median and ninety-fifth-percentile time from report to authenticated dispatch;
- acknowledgement and preservation time by priority;
- proportion of positive matches confirmed, rejected or unresolved after review;
- false-association and correction rates;
- records preserved before ordinary expiry;
- time from correction to complete propagation;
- query breadth and protected-category use;
- refusal reasons and resolution;
- provider hours and cost per completed journey;
- security incidents and critical findings;
- user comprehension of evidence class and confidence;
- partner onboarding time and conformance;
- cost against baseline and forecast.

[45] Cloud Security Alliance, *Cloud Controls Matrix v4.0.12* (2024); ISO/IEC 19941:2017, *Cloud Computing—Interoperability and Portability*; NIST, *Cloud Computing Reference Architecture* (n 44).

[46] Government Digital Service, 'Service Standard' (n 23); Cabinet Office, 'Technology Code of Practice' (n 23); National Audit Office, *Digital Transformation in Government: Addressing the Barriers to Efficiency* (10 March 2023).

The programme should not publish a target number of attributions. Such a target rewards labelling. It should publish whether evidence survived, whether uncertainty was represented and whether action became faster.

Counterfactual evaluation is difficult. For sampled cases, independent reviewers should ask what the ordinary route would probably have taken and whether the relevant record would have remained. Comparison with similar pre-pilot cases can provide a range. Claims that MOSAIC “prevented” a catastrophe require a causal account.

10. Failure Conditions and Objections

The strongest objection is that a federation of sensitive indexes creates the surveillance and espionage instrument it claims to resist. That objection is not answered by benevolent purpose. Local custody, case-bound query, protected-category review, minimum disclosure, oversight and revocation reduce the risk; they do not remove it. A State unwilling to submit its own node to these controls should not receive broad access to others.

A second objection is that hostile States will remain outside. They may. MOSAIC is still useful where contractors route through commercial services, allied jurisdictions and States which prefer not to be unwitting hosts. The system should not be sold as global. Route-around data will show whether extension changes coverage.

A third is that sophisticated attackers will alter indicators. The protocol is not dependent upon one address. Temporal, behavioural, account, payment, manifest and provider links may combine. Yet evasion will occur. The measure of success is improved evidence and speed, not perfect visibility.

A fourth is that privacy-preserving matching will be expensive, slow or falsely reassuring. The design therefore begins with exact queries, uses advanced techniques where their threat model justifies them and retains lawful conventional process. Cryptography should solve a defined disclosure problem, not decorate procurement.

A fifth is cost. The core programme costs more than a conventional threat-sharing platform because it includes twenty-four-hour security, legal process, evidential continuity, oversight and international adoption. Removing those elements produces a cheaper product which does not answer the paper’s problem. The staged gates permit Parliament to reject the cost after evidence.

A sixth is constitutional mission creep. A preservation service may become production; defensive correlation may become domestic intelligence; a manifest may become prior licensing of every security test. Powers, roles, protected categories, transparency, review and sunset must therefore be statutory. Architecture cannot substitute for law.

A seventh is false confidence. A colourful graph joining twelve jurisdictions may persuade a minister beyond the evidence. The interface must retain contrary hypotheses, source classes and separate confidence. Training and independent analytic review are as important as algorithm.

An eighth is evidential incompatibility. What helps a defender may not satisfy a criminal court. MOSAIC does not promise one record for all purposes. It preserves provenance and allows each forum to apply its rules. A failed prosecution does not necessarily erase a defensive observation; a secret assessment cannot alone satisfy a public criminal burden.

A ninth is provider burden. Unfunded integration would favour hyperscale providers and penalise small firms. Reference software, hosted gateways, staged duties, reimbursement and simple interfaces

distribute cost. Providers should participate in design but not receive a veto upon necessary public protection.

A tenth is sovereignty. A foreign query may be felt as intrusion. The system’s answer is that custody and legal decision remain national. If the request lacks authority, the node refuses and records why. The protocol makes the boundary visible.

Finally, MOSAIC may be compromised. The architecture is designed upon that assumption. A compromised node is isolated; signed objects are revalidated; keys rotate; correction propagates; manual channels remain; and the incident is reported. The alternative—treating compromise as unthinkable—would leave the federation unable to recover from the event most likely to test it.

11. Conclusion

Jurisdiction by design is effective because computation moves faster than public law and because every custodian sees too little. The answer cannot be to deem each territorial State omniscient. It must be to preserve the fragment, correlate it lawfully and require the controller which possessed the map to keep an accountable record.

MOSAIC makes that proposition operational. Evidence remains local until law permits production. Signed federated queries discover relationships. Emergency notices preserve identified material. Source classes distinguish observation from allegation and attribution. The manifest records who authorised, controlled and changed a distributed operation. Corrections travel as far as errors. Human authorities remain responsible for coercion and legal judgement.

The recommended core programme costs an estimated £61.2 million over three years, following a £10.61 million pilot, with explicit contingency and gates. That is a substantial sum. It is not substantial beside one severe winter-grid interruption, the destruction of irreplaceable health data or the strategic cost of responding against the wrong actor. Cost alone does not prove value; the pilot measures whether time, preservation and evidential quality improve.

The protocol will not compel an adversary to confess. It will deprive willing jurisdictions, providers and controllers of the excuse that cooperation necessarily begins after deletion. It will also make refusal visible, so that due diligence can be judged upon what a State knew, could do and chose.

Law frequently arrives after a new means of power has become ordinary. Here the delay is part of the weapon. A legal doctrine which recognises fragmentation but supplies no instrument leaves the attacker’s most decisive advantage untouched. MOSAIC is the instrument: limited enough to remain lawful, fast enough to preserve the fact, and rigorous enough that retaliation, restraint or prosecution may rest upon evidence whose path can be shown.

Bibliography

Books, Chapters and Articles

Benny Pinkas, Thomas Schneider and Michael Zohner, ‘Faster Private Set Intersection Based on OT Extension’ (23rd USENIX Security Symposium 2014) 797

Evelyne Schmid and Ayşe Özge Erceiş, ‘The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility’ (2023) 33 *Swiss Review of International and European Law* 577, 581–90

Jon Lindsay, ‘Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack’ (2015) 1 *Journal of Cybersecurity* 53, 53–67

Kallista Bonawitz and others, ‘Practical Secure Aggregation for Privacy-Preserving Machine Learning’ (Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security 2017) 1175, 1175–91

Kristen Eichensehr, ‘The Law and Politics of Cyberattack Attribution’ (2020) 67 *UCLA Law Review* 520

Lea Kissner and Dawn Song, ‘Privacy-Preserving Set Operations’ in Victor Shoup (ed), *Advances in Cryptology—CRYPTO 2005* (Springer 2005) 241

Santiago Torres-Arias and others, ‘in-toto: Providing Farm-to-Table Guarantees for Bits and Bytes’ (28th USENIX Security Symposium 2019) 1393

Michael Freedman, Kobbi Nissim and Benny Pinkas, ‘Efficient Private Matching and Set Intersection’ in Christian Cachin and Jan Camenisch (eds), *Advances in Cryptology—EUROCRYPT 2004* (Springer 2004) 1

Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) rr 69 and 71

Sarah Brown, Joep Gommers and Oscar Serrano, ‘From Cyber Security Information Sharing to Threat Management’ in WISCS ’15: *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security* (ACM 2015) 43

Thomas Rid and Ben Buchanan, ‘Attributing Cyber Attacks’ (2015) 38 *Journal of Strategic Studies* 4, 4–37