

分析性工作论文

数据使馆与沙特主权连续性：一个可检验的比较框架

一份基于公开资料的分析工作论文，用比较案例、法律边界、技术分层和可检验命题，评估数据使馆何时可能增强沙特的主权连续性。

文章日期

2026年10月18日

作者

Safwan AlModhayan

关键词: 数据使馆 · 主权连续性 · 数字主权 · 门限密码学 · 政府连续性 · 风险治理

本文是由作者文章与截至2026年10月18日的公开资料衍生的分析工作论文。它未经同行评议，不构成法律意见，也不报告已经实施的实验或实际政府项目结果。

isafwan.com/zh-CN/research/data-embassies-sovereign-continuity/

摘要

本文考察数据使馆（Data Embassy）何时能作为沙特主权连续性（Sovereign Continuity）的一部分发挥作用。研究采用公开资料的比较性文件分析，区分档案保存、灾难恢复、政府连续性与可证明的公共职能输出。^[1]

核心结论是：境外受保护副本只解决连续性的一部分。软件、身份、签名、通信、合法授权、人员以及独立恢复路径仍决定国家能否把数据转化为服务。地理冗余若共享身份、密钥、管理或法律风险，仍会遭遇共模失效（Common-Mode Failure）。

本文提出分层架构、风险矩阵、可检验命题与阶段性试点，而不报告未经实施的结果。任何沙特应用都须服从数据分类、目的、国内法律、主管机关决定、东道国法律以及具体架构事实；长期资产还应具备密码敏捷性（Cryptographic Agility）。^[16]

研究问题

主要问题是：在什么法律、技术和运行条件下，境外托管安排能够降低沙特关键公共职能的中断风险，而不把控制权转移给单一东道国、供应商或管理员？

子问题包括：哪些职能值得保护，数据位置与实际控制如何区分，如何分配密钥与恢复权限，如何测量恢复时间目标（Recovery Time Objective, RTO）和恢复点目标（Recovery Point Objective, RPO），以及如何验证退出能力。

本文不判断某一具体沙特项目合规，不提出秘密设施位置，不估算武装冲突概率，也不把比较案例写成通用因果证明。它提供的是供试点验证的问题结构。

方法与案例选择

研究采用文件比较法，材料包括双边协议、法院判决、政府陈述、监管文本、技术标准、同行评议论文及机构报道。每项事实只在来源可支持的范围内使用，并将官方战时说法与独立审计区分。

案例按功能选择：爱沙尼亚说明法律托管机制，乌克兰说明战时迁移的官方说法，克什米尔与叙利亚说明记录对权利证明的作用，苏丹说明档案与通信双重脆弱，ICARDA说明从保存到再生的转换。^{[1] [2] [3] [4] [5] [6] [7] [8] [9]}

这种选择不是国家排名，也不能估计事件发生率。分析把案例转化为可测试要求，并明确公开资料无法给出沙特成本、性能与合规结论。

概念界定

数据使馆是受专门法律安排保护的境外计算、档案与系统托管场所；它不是自动获得外交领土性质的数据中心。主权连续性指国家在多点压力下继续运行选定职能并验证输出，同时保持合法决策与密码控制。

灾难恢复（Disaster Recovery）关注系统资源的恢复；政府连续性（Continuity of Government）关注治理职能；数据溯源（Provenance）记录数据来源与变换；完整性（Integrity）说明副本未被未经授权改变，却不自动证明原始事实为真。

共模失效是多个冗余方案因同一依赖而同时失效。NIST把冗余方案对共同原因的脆弱性与多样性原则联系起来；因此“地点不同”不能替代对身份、密钥、管理、通信和法律依赖的审查。^[10]

比较发现

爱沙尼亚—卢森堡安排证明，法律保护来自明确双边协议，而不是“使馆”名称；协议保留适用法律、争议、退出和代表机制。^[1]

乌克兰官方材料表明，境外云资源可以在物理站点遇袭时支持关键登记册，但该陈述不是逐系统独立审计。克什米尔、叙利亚与苏丹显示，记录遗失会直接进入权利、财产和救援，而通信中断又能让完好数据库失去社会可达性。^{[3] [4] [5] [6] [7]}

ICARDA从斯瓦尔巴取回样本并在黎巴嫩、摩洛哥再生，说明连续性要求从被保存的对象重建实际功能。这些案例共同支持“以职能为起点”的设计，却不能证明单一架构适合所有领域。^[8]

法律框架

2017年协议赋予托管场所免受搜查、扣押与执行等保护，进入原则上须经爱沙尼亚授权代表事先同意；只有火灾或其他需要立即采取保护措施且危及安全的紧急情形，才推定同意。第六条把所有数据和系统视为爱沙尼亚档案，保护官方通信并允许使用密码和加密。第八条则保留国际法、欧盟法以及在适用时的卢森堡法，并规定仲裁。服务器没有因此成为爱沙尼亚领土，《维也纳外交关系公约》也不会自动创设这种地位。^[1]

终止在通知24个月后生效，资产交给获授权代表；无法确认时，按卢森堡档案标准保护并只交给爱沙尼亚合法代表。这些条款表明，进入、争议、退出和代表资格必须在危机前确定。^[1]

在沙特语境中，个人数据境外传输仍须服从国家安全与重大利益、最低必要范围、适当保护、个人权利，以及充分性评估、适当保障或法规列明的特定例外；持续或大规模敏感传输等情形还需要风险评估。国际协议可能是主管机关依法评估后采用的一条路径，却不是机构自行启动传输的授权。云计算网络安全控制（Cloud Cybersecurity Controls, CCC）只是在其范围内适用的安全框架，不能取代个人数据保护制度、信息分类或行业要求。^{[14] [15]}

技术框架

技术层必须区分三类工具：认证加密（Authenticated Encryption）保护机密性并暴露篡改；纠删码（Erasure Coding）把加密内容分成若干片段，使足够数量的片段在部分丢失后仍可重建内容；门限密码学（Threshold Cryptography）分散密钥或密码操作的权限。混淆三者，会让某一层被误认为能够完成它并不承担的功能。

沙米尔秘密共享 (Shamir's Secret Sharing) 在正确数学模型中允许达到门限的份额恢复秘密，低于门限的份额不泄露秘密。“五取三”说明可以失去两份，但它不证明数据可用、恢复授权正确，也不证明承载份额的计算机安全。实际系统还需托管人独立、份额防盗防替换、定期轮换和监控，并演练更换失联或不再可信的托管人。^[11]

多方计算 (Multi-Party Computation, MPC) 和门限签名 (Threshold Signatures) 可以在不把完整密钥集中到一处的情况下执行操作，并可配合硬件安全模块 (Hardware Security Modules, HSMs)。但协议复杂度会增加审计与事件响应负担。还应把保存、备用运行、身份、签名、监控和通信分层测试，建立独立管理路径、供应商切换、密钥轮换与受控降级模式 (Controlled Degraded Mode)。评价标准不是技术是否新颖，而是它能否在机构最差运行条件下减少某项明确风险。

完整性、溯源与事实真实性

密码哈希 (Cryptographic Hash)、默克尔树 (Merkle Tree) 或防篡改日志 (Tamper-Evident Log)，可以证明与已记录指纹关联的副本没有在不留痕迹的情况下改变；它们不能自动证明最初录入的事实正确。恢复判断必须分别回答：原始输入是否正确，保存副本是否完整，变更是否由合法权限发起。

无密钥签名基础设施 (Keyless Signature Infrastructure, KSI) 的供应商文件称其可以验证签名时间、数据完整性、顺序与输入指纹。该材料来自技术供应商，因此可说明产品宣称的证据范围，却不能充当对历史事实、法律正确性或全部营销主张的独立验证。^[12]

可信恢复需要独立保存哈希锚点、授权记录和审计证据，并能依靠数据溯源确认哪一份副本已知安全、谁以何种权限修改了它、需要回退哪些变更。人工智能参与录入与变更后，数据投毒 (Data Poisoning)、身份冒充和自动化可能把错误迅速传播到所有副本，这使三层分离更为重要。

恢复授权模型

模型应区分政策决定、密码执行、备用运营和独立审计。职能所有者决定什么必须恢复；合法机关触发程序；密钥托管人只执行达到门限的密码操作；备用运营者在限定范围内恢复服务。

继任顺序、最低同意数、异议、紧急权限期限、跨境联系和事后审查都应书面化。任何单一角色都不应同时决定恢复、持有全部密钥并确认自身操作正确。

门限授权 (Threshold Authorization) 不能只存在于密码层，还需与法律权限、可验证身份和审计路径对应。否则系统可能在数学上安全，却在制度上无权启动。

风险矩阵

风险矩阵应按场景记录发生可能性、影响、现有控制、剩余风险、触发条件、发现方法、恢复路径和关闭测试所需证据。它不是一张把所有格子涂绿的合规表。

场景可包括失去两个站点、国际链路中断、东道国突发法律限制、共同管理界面失效、密钥份额被盗、错误删除同步扩散、恢复请求冲突以及加密算法无法迁移。

矩阵还要分别呈现机密性丧失、可用性丧失、证据污染和合法权限被滥用。提高门限可能降低单点接管风险，却延长恢复并增加人工失败，因此控制之间也需权衡。

可检验命题

命题一：地理分布只有同时覆盖身份、密钥、管理和通信依赖，才会缩短停机。可比较“多地点但统一管理”和“具有备用身份及管理路径”的恢复演练。

命题二：分散密钥权限会降低单人接管风险，却可能增加恢复时间与人工程序失败。应改变门限、托管人数和缺席条件，测量授权时间、错误与拒绝请求，而不预设“五取三”最佳。

命题三：可验证溯源能在篡改事件后缩短识别安全副本的时间，前提是信任锚与授权日志独立于受损系统。命题四：预先定义的受控降级运行，可能比完整系统恢复更快提供有用公共输出。

这些命题不包含结果。测试可能表明复杂性抵消收益，某职能不适合境外托管，或独立国内路径更便宜稳定；试点的价值就在于允许这些答案出现。

经济评估框架

评估应比较全生命周期成本与中断成本。前者包括建设、连接、演练、培训、审计、合同、密钥轮换、算法迁移和退出；后者包括交易损失、人工工作、权利延误、信任修复与对其他机构的外溢。

可用匿名化内部事件与测试建立基线，测量恢复时间、数据损失、人工工时和切换成本。单次战争或市场波动不能直接变成固定财务系数。

供应商与东道国锁定也应定价：法律或合同变化后，提取可用格式的数据、密钥和日志需要多久、花费多少。定期退出测试比从未演练的合同条款更能反映真实成本。

可检验的评估标准

第一项是功能：每项关键服务都定义公民或机构可以实际使用的最低输出。时间指标采用恢复时间目标（Recovery Time Objective, RTO）与恢复点目标（Recovery Point Objective, RPO），分别衡量不可接受影响前的最长停机和可回退时间点所代表的可承受数据损失。^[13]

第二项是独立性：在失去预定站点、托管人、供应商或共同身份服务时仍能恢复，并统计发现的共同依赖。第三项是恢复完整性：服务恢复前能识别被污染或未授权的副本，并证明所选副本的数据溯源。

第四项是权限正确：低于门限或来自未获授权主体的请求不会执行，并且负责人缺席时，既定继任顺序能够工作。第五项是退出可行：数据、密钥、软件和审计记录可以在已知时间与成本内迁移到另一托管方。第六项是合规：在引入真实数据前，能够证明分类、目的、法律依据、数据最小化和主管机关决定。这些是建议指标，本文并不声称任何尚未实施的系统已经通过。

分阶段试点设计

第一阶段用合成数据（Synthetic Data）和非敏感服务模拟真实政府职能，绘制依赖、设定RTO与RPO，并建立加密保存、备用运行、分布式密钥和审计日志。能不用真实个人数据验证的概念，就不应先使用真实数据。

第二阶段在独立监督下进行复合故障演练：站点丢失、托管人缺席、通信中断、污染副本、未授权请求和供应商切换，并记录时间、决策、人工失败和理论图中遗漏的依赖。

只有在独立法律、技术与隐私审查完成、重大缺陷关闭且退出能力得到证明后，才考虑更高敏感度的数据或职能。试点得出某类数据不宜境外托管，同样也是有效结果。

实施与治理考量

治理需要职能所有者，而不只是存储所有者。业务机构理解记录丢失的后果，数字部门管理集成，网络安全部门测试防御，监管机构审查跨境与隐私，外交部门协商法律地位；风险接受责任应明确书面归属。

合同应包括审计权、事件通知、处理地点和分包商、资产返还与副本销毁、迁移协助，且合规证据不能只由供应商自证。国家间协议则处理进入、扣押、通信、适用法律、争议、终止和代表资格。

长期资产需要密码敏捷性（Cryptographic Agility）：算法、证书与密钥清单，以及轮换和重新加密计划。NIST在2024年8月批准FIPS 203、204和205，并不证明现有密码已崩溃，却说明算法迁移应在危机前成为可运行能力。^[16]

局限与不确定性

部分案例来自政府或媒体陈述，未公开完整运行日志。公开资料不能确认乌克兰每项服务的可用性、苏丹每份档案的状态，或每次中断对所有用户的影响。

把法律档案、种子和政府系统并置，只是有限的功能比较，并非物理等同。沙米尔方案的数学保证不等于实现安全；KSI供应商材料也不证明原始数据真实或所有爱沙尼亚服务普遍采用。

本文没有沙特项目的成本数据、性能测量或合规评估。地缘政治与法律风险还会随时间变化，任何实施决定都需当时的威胁建模、分类、测试、合同与独立审查。

案例选择受可得性偏差影响：政府、法院和媒体记录的事件更容易研究。公开成功可能隐藏次要服务故障，公开失败也可能只是透明度更高，因此本文不以案例数量给国家排名或估计失败率。

结论

数据使馆可以是更大架构中的工具，却不是架构本身。协议提供名称无法创造的法律保护，真正独立的地点、管理和密钥分布也能抵抗部分故障；但没有软件、身份、通信、签名与授权，数据仍不会自动变成公共职能。

可辩护的沙特框架应当选择性部署、先经测试、从职能出发：明确可承受的停机与损失，分离权限与持有，把溯源和授权正确性纳入恢复，并使所有跨境动作受法律与主管机关控制。

战略价值不在数据使馆数量或存储容量，而在一个可证明的答案：失去若干站点、通信和密钥托管人之后，国家还能否以合法决定，在社会可承受的时间内证明正确权利并运行最低必要服务？

主权连续性闸门 (Sovereign Continuity Gates)

1	2	3	4
恢复时间目标 (Recovery Time Objective, RTO) 与恢复点目标 (Recovery Point Objective, RPO)	对共模失效 (Common-Mode Failure) 的法律与技术独立性	具有合法门限的分布式授权 (Threshold Authorization)	通过可验证数据溯源 (Provenance) 完成的恢复演练

模型只有通过四道闸门，才应进入真实数据阶段：明确职能、降低共同依赖、确认权限正确，并在可接受的时间和数据损失范围内证明恢复完整。

参考文献

1. Agreement between Estonia and Luxembourg on the hosting of data and information systems
Riigi Teataja, 2017年6月20日
2. The Legal Status of Data Embassies
International and Comparative Law Quarterly, 2019年1月1日
3. Ukraine's cybersecurity infrastructure protected state registers during the war
President of Ukraine, 2022年9月6日
4. Farooq Ahmad Dar v. State of Jammu and Kashmir
High Court of Jammu and Kashmir and Ladakh, 2022年4月13日
5. Q&A: Syria's New Property Law
Human Rights Watch, 2018年5月29日
6. 30 million Sudanese historical documents at risk of deterioration
Asharq Al-Awsat, 2026年6月26日
7. Sudan telecommunications joint statement
Norwegian Refugee Council, 2024年5月3日
8. ICARDA seeds safe back in Lebanon and Morocco
Svalbard Global Seed Vault, 2017年10月27日
9. Norges tilstedeværelse i Storbritannia under 2. verdenskrig
National Archives of Norway

10. Engineering Trustworthy Secure Systems
NIST, 2022年3月1日
11. How to Share a Secret
Communications of the ACM, 1979年11月1日
12. KSI Technology
Guardtime
13. Contingency Planning Guide for Federal Information Systems
NIST, 2010年5月1日
14. Implementing Regulations for Personal Data Transfer outside the Kingdom
SDAIA
15. Cloud Cybersecurity Controls CCC – 2:2024
National Cybersecurity Authority
16. NIST Releases First 3 Finalized Post-Quantum Encryption Standards
NIST, 2024年8月13日