COSMOS LOCK Partner Brief

Separate reconstruction control for sensitive personal data

We propose an OEM module that lets an enterprise retain control over reconstruction information while delegating data storage. Its goal is to prevent storage authority alone from enabling bulk plaintext reconstruction, while keeping approved single-record and multi-record work usable.

Start with selected sensitive fields in one existing workflow. Connect through an API or SDK adapter and retain familiar screens and identity systems. This is a productization architecture proposal requiring implementation and validation in the intended operating environment.

Customer value and first application

The first fit is an enterprise that needs different administrators for storage operations and sensitive-data reconstruction. A customer-service workflow, for example, can retrieve approved customer details in batches while the enterprise controls the permitted records, fields and cumulative volume.

Proposed architecture

Component	Responsibility
Data storage domain	Stores authenticated encrypted fragment pages. Holds no coordinate maps, internal decryption keys or authority to grant reconstruction.
Customer control service	Controls encrypted coordinate maps, key use, policy and cumulative usage. Reconstructs approved data inside its protected execution boundary.
Application adapter	Passes verified identity and requested records and fields. Receives approved results; never receives raw maps or internal keys.

Administrative, deployment and backup permissions must preserve this separation. Protection assumes that the customer control service and reconstruction runtime remain protected. A compromised authorized application may expose its permitted results; input copies and plaintext already delivered need separate protection.

Patent foundation

The engine retains actual data division, random coordinate assignment, coordinate separation and associated data or arrangement information. US 12,411,980 claims 1 and 5 are the core mapping basis; “at least one” includes both single and multiple originals. Claim-specific additions and product controls are mapped separately.

Patent text: https://patents.google.com/patent/US12411980B2/en#C

Validation and partner collaboration

Normal work with controlled reconstruction

The target design batches authorization and page reads, reuses decrypted pages within a request and updates affected pages and maps. Compact coordinates and connection reuse aim to reduce overhead. Interactive work and scheduled bulk jobs use separate resource budgets, with cumulative limits across chunks.

Routine work follows existing permissions without repeated manual approval. Each request checks current permissions and cumulative reconstruction volume. The design keeps revoked permissions from becoming valid again after a service restart. These are target operating controls requiring implementation and validation.

Plaintext lifetime and incident response

Customers set maximum use periods and idle limits by workflow. Within managed execution and integrated applications, task completion, expiry or cancellation triggers cleanup of temporary plaintext and ends further use under that grant. Stored protected records remain available for newly authorized reconstruction.

Implementation must address memory copies, caches and failure paths. Copies already exported or captured cannot be recalled. Incident signals can suspend subsequent reconstruction. Optional AI integration should prefer masked data or approved action results, with delegated agents sharing the original job’s limits.

Optional NEXAUTH step up

NEXAUTH is proposed for separately evaluated high-risk requests, such as expanded reconstruction scope or exceptional export. Relationship context must come from trusted evidence and an independent confirmation path.

A defined first collaboration

Stage	Deliverable and decision
Technical fit	One product, workflow and adapter. Agree integration needs, control boundaries and the engineering scope.
Scoped PoC	Agree security boundaries, workload SLOs, recovery and total cost. Validate real separation, persistent controls and concurrent performance against equivalently controlled alternatives.
Productization	Proceed when customer benefit supports deployment. Agree engineering ownership, OEM scope, support and licensing.

The first evaluation will assess security boundaries, accuracy, workload performance, cleanup and recovery. Production readiness and customer benefit must be established for the selected deployment.

We propose a fixed-scope paid or cost-shared PoC, followed by a deployment-based annual license and support. Agree engineering resources, ownership and responsibilities before work.

Next step: identify one sensitive-data workflow and review its integration requirements.

COSMOS LOCK 파트너 브리프

민감 개인정보를 위한 별도 복원통제

기업이 데이터 저장 운영을 위임하면서도 복원정보는 직접 통제하는 OEM 모듈을 제안합니다. 저장영역의 권한만으로 원문을 대량 복원하지 못하도록 하고, 승인된 단건·다건 업무는 이용에 불편하지 않은 수준으로 처리하는 것이 목표입니다.

기존 업무 하나의 민감한 개인정보 필드부터 적용합니다. API 또는 SDK 어댑터로 연결하고 익숙한 화면과 인증체계를 유지합니다. 현재 제품화 아키텍처 제안 단계이며, 적용 환경에 맞춘 구현과 검증이 필요합니다.

고객 가치와 첫 적용 업무

저장 운영과 민감정보 복원을 서로 다른 관리자가 통제해야 하는 기업을 우선 대상으로 합니다. 예를 들어 고객 상담 업무에서 승인된 고객 상세정보를 다건 조회하되, 도입 기업이 허용할 원본·필드·누적 복원량을 결정하는 구성입니다.

제안 아키텍처

구성	역할
데이터 저장영역	인증 암호화된 조각 페이지를 보관합니다. 좌표맵·내부 복호화키·복원권한 발급 권한을 갖지 않습니다.
고객 복원통제 서비스	암호화된 좌표맵, 키 사용, 정책과 누적 사용량을 통제합니다. 보호되는 실행 경계 안에서 승인된 원문을 복원합니다.
업무 어댑터	검증할 신원과 요청 원본·필드를 전달하고 승인된 결과를 받습니다. 원시 좌표맵과 내부키는 전달받지 않습니다.

관리자·배포·백업 권한까지 분리 구조를 유지해야 합니다. 고객 복원통제 서비스와 복원 실행영역이 보호된다는 조건에 의존합니다. 권한 있는 앱이 침해되면 허용된 결과가 노출될 수 있으며, 입력 원본 사본과 이미 전달된 평문에는 별도 보호가 필요합니다.

특허 기반

실제 원본 분할, 랜덤 좌표 부여, 좌표 분리와 데이터정보 또는 배치정보 연결을 기본 엔진에 유지합니다. 미국 12,411,980 의 1 항·5 항을 핵심 대조 기준으로 삼으며, ‘적어도 하나’는 단건과 복수 원본 모두를 포함합니다. 청구항별 추가 구성과 제품 운영통제는 구분해 대조합니다.

등록청구항: https://patents.google.com/patent/US12411980B2/en#C

검증과 파트너 협력 제안

정상 업무와 복원통제를 함께 유지

목표 설계는 권한 확인과 페이지 읽기를 묶고, 같은 요청 안에서 해독한 페이지를 재사용하며, 변경된 페이지와 맵만 갱신합니다. 짧은 좌표와 연결 재사용으로 비용을 줄이고, 일반 조회와 예정된 대량 작업의 자원을 분리합니다. 대량 작업을 작은 묶음으로 처리해도 작업 전체의 누적 한도를 유지합니다.

일상 업무는 기존 권한에 따라 반복 수동 승인 없이 처리하고, 요청마다 현재 권한과 누적 복원량을 확인하고, 서비스가 재시작돼도 취소된 권한이 다시 허용되지 않도록 합니다. 이것은 구현·검증 대상입니다.

원문 사용시간과 사고 대응

고객이 업무별 최대 사용시간과 미사용 한도를 설정합니다. 관리되는 실행영역과 연동 앱에서 업무 완료·기한 만료·취소 시 임시 원문을 정리하고 해당 사용권한을 종료하도록 설계합니다. 보호된 저장 원본은 유지하며, 다시 필요하면 현재 권한을 확인해 복원합니다.

메모리 사본·캐시·오류 경로까지 구현 검증이 필요하며, 반출·캡처된 사본을 회수할 수는 없습니다. 사고 신호로 후속 복원을 중단하고, 선택적 AI 연동은 마스킹 정보나 승인된 행위의 결과를 우선 제공합니다. 하위 에이전트도 원래 작업의 한도를 공유합니다.

NEXAUTH 선택형 추가 인증

복원 범위 확대나 예외 반출 등 고위험 요청에 NEXAUTH 를 별도 평가하는 옵션으로 제안합니다. 관계성 맥락은 신뢰할 수 있는 근거와 독립된 확인 경로로 검증해야 합니다.

첫 협력의 범위

단계	산출물과 판단
기술 적합성 검토	제품·업무·어댑터 각 하나를 선정하고 연동 요구사항·통제 경계·개발 범위를 검토합니다.
범위가 정해진 PoC	보안 경계·업무 성능·복구·총비용을 합의합니다. 실제 권한 분리, 영속 통제, 동시 성능을 동등한 통제의 대안과 비교합니다.
제품화	도입을 정당화할 고객 이익이 확인되면 개발 주체·OEM 범위·지원·라이선스를 합의합니다.

첫 평가에서는 보안 경계·정확성·업무 성능·원문 정리·복구를 확인합니다. 선택한 배포 환경에서 상용 준비 수준과 고객 이익을 검증하는 것이 협력의 목표입니다.

범위가 고정된 유상 또는 비용분담 PoC 후 배포 단위 연간 라이선스·지원을 협의하는 모델입니다. 개발 자원·소유권·역할은 착수 전에 합의합니다.

다음 단계는 민감정보 업무 하나를 선정하고 연동 요구사항을 함께 검토하는 것입니다.