/

WHITEPAPER · EMNA · MAI 2026

Das eingefrorene Gespräch

Die bisher ungegebene Möglichkeit in der Notfall- und Nachlassvorsorge.

M.I.A. | ZERO-KNOWLEDGE | PATENT ANGEMELDET | MADE IN GERMANY

01 Die Lücke, die niemand sah und schloss
Was Testament, Vollmachten, Passwort-Manager und Plattform-Nachlass leisten – und was nicht.

02 Das eingefrorene Gespräch
Über das Gespräch, das die meisten nie führen – und warum emna es in Mathematik verwandelt.

03 Das M.I.A.-Verfahren – Die Architektur unter der Haube
Mathematical Immutable Access (M.I.A.) kennt keine Logins und Berechtigungslogik.

04 Das Patent – die unsichtbare Innovation
Worum es bei M.I.A. wirklich geht – und wo die Erfindung beginnt.

05 Vergleichsmatrix – was emna ergänzt
Warum emna kein Ersatz für bestehende Instrumente ist – sondern die Schicht, die bisher fehlte.

06 Fallbeispiel – ein Vorsorge-Fall in 30 Sekunden
Zwei QR-Codes scannen. Alle Informationen verfügbar. Keep it simple and stupid.

07 Fazit
emna und M.I.A. – jeweils selbstständig und gemeinsam hervorstehend stark.

Herausgeber: Sacom EDV GmbH · emna.app
Adressaten: Datenschutzverantwortliche, Juristen, CIOs, Sicherheitsberater, Entwickler, interessierte Mandanten
Stand: Mai 2026 · Version 1.0

01 Die Lücke, die niemand sah und schloss

Was Testament, Vollmachten, Passwort-Manager und Plattform-Nachlass leisten – und was nicht.

Vorsorge besteht heute aus Inseln, die nichts voneinander wissen.

Das Testament regelt, wer erbt – aber es wird vor allen Erben verlesen, weit nach dem Tod. Individuelle Nachrichten, vertrauliche Zugänge oder situationsabhängige Anweisungen haben darin keinen Platz. Die Patientenverfügung regelt medizinische Entscheidungen – aber nicht, wer sich wie um die Kinder kümmert, wo die Versicherungspolice liegt, welche Daueraufträge laufen oder das Unternehmen weitergeführt werden soll.

Große Plattformen bieten Nachlasskontakte an – aber nur für deren eigene Kontodaten, nur im Todesfall, und nur innerhalb des jeweiligen Ökosystems. Passwort-Manager speichern Zugänge, aber kennen keine Situationen, keine unabhängige Prüfung und keine persönlichen Botschaften. Inaktivitäts-Mechanismen lösen nach Ablauf einer Frist aus – ohne menschliche Prüfung, mit dem Risiko der Fehlauslösung. Und der Zettel im Tresor ist veraltet, bevor die Tinte trocken ist.

Was fehlt, ist eine Lösung, die das alles zusammenbringt und rechtliche Dokumente sogar juristisch korrekt ergänzen kann:

- Situationsbasierter Zugriff – nicht nur Tod, sondern auch Koma, Handlungsunfähigkeit, Verschollenheit, etc.
- Pro Eintrag, pro Person, pro Situation – mathematisch getrennt, nicht öffentlich wie ein Testament
- Menschliche Prüfung durch einen unabhängigen Dritten – Anwalt/Notar, statt Algorithmus
- Plattformunabhängig – alles an einem Ort, egal woher die Information stammt
- Persönliche Botschaften, Videos, Zugänge, Dokumente und Anweisungen – zusammen, an einem Ort
- Kryptographisch erzwungene Zugriffskontrolle – nicht durch Programmlogik, sondern durch Mathematik
- Post-Quantum-Verschlüsselung – sicher auch gegen zukünftige Technologien
- Zero-Knowledge – niemand außer die Berechtigten können Daten lesen

> Es gab keine Lösung, die das alles vereint. Das sind die Lücken, die emna schließt und jegliche Vorsorge komplettiert.

02 Das eingefrorene Gespräch

Über das Gespräch, das die meisten Menschen nie führen – und warum emna es in Mathematik verwandelt.

Die meisten Menschen führen ein Gespräch nie: Was soll mit meinen Zugängen, Dokumenten Kindern, Unternehmen und Anweisungen passieren, wenn mir etwas zustößt? Was sollen meine Kinder wissen? Was mein Partner? Was mein Geschäftspartner? Und was davon erst im Todesfall – und was schon bei einem Koma?

emna ersetzt dieses Gespräch. Die App folgt einem einfachen Schema: Einträge anlegen, Berechtigte bestimmen, Situationen festlegen. So einfach wie einen Brief zu schreiben – aber jederzeit änderbar, weil sich das Leben ändert. Und nicht nur für den Tod, sondern für jede Situation, in der man plötzlich nicht mehr handlungsfähig ist.

Was dabei im Hintergrund passiert, bekommt der Nutzer kaum mit. Bei der Einlagerung entsteht aus seinen Einträgen eine kompilierte, verschlüsselte Datenbank – ein geschlossenes Artefakt. Es wird beim Betreiber verwahrt, wie eine Jacke an der Garderobe. Der Betreiber nimmt sie entgegen und gibt sie im Ernstfall heraus. Aber er kann sie nicht öffnen – die Knöpfe sind verschlossen. Und obwohl es nur eine einzige Datei ist, enthält sie für jede Situation und jeden Berechtigten mathematisch getrennte Pfade – wer für eine bestimmte Situation bestimmte Einträge nicht erhalten soll, kann ihn nicht lesen. Nicht durch Manipulation, nicht durch Technik, nicht durch Autorität.

Es gibt keinen Login zur eingelagerten Datenbank. Kein Admin-Panel. Keine API. Was beim Betreiber liegt, ist eine Datei, die ohne die richtigen Schlüssel nicht von Zufallsdaten zu unterscheiden ist. Und trotzdem entscheidet am Ende nicht ein Algorithmus über die Freigabe, sondern ein Mensch – ein Anwalt, der prüft, ob die Situation eingetreten ist.

> Das ist das „eingefrorene Gespräch": Ein Gespräch, das die meisten nie führen – transportiert in ein Erzeugnis, das im Moment der Einlagerung für immer so eingefroren wird, wie der Ersteller es bestimmt hat. Ohne Login, ohne Cloud. Nicht umprogrammierbar, nicht aufschließbar, nicht verhandelbar. Kein Versprechen – Mathematik. Und sollte sich die Technik weiterentwickeln, genügt eine neue Einlagerung, um den Schutz für die nächsten Jahrzehnte zu aktualisieren.

03 Die Architektur unter der Haube – Das M.I.A.-Verfahren

Mathematical Immutable Access (M.I.A.) kennt keine Logins und Berechtigungslogik

Hinter **emna** steht das Verfahren mit dem Namen M.I.A. – *Mathematical Immutable Access*. Der Name beschreibt eine Eigenschaft, die in der digitalen Welt bislang nicht selbstverständlich war: Zugriff entsteht nicht durch eine Software-Regel, sondern durch eine mathematische Konstellation. Wer die Konstellation hat, kann lesen. Wer sie nicht hat, scheitert unwiderbringlich.

Drei Teile, drei Parteien

M.I.A. teilt das System auf drei Parteien auf, die jeweils nur einen Teil dessen halten, was zur Entschlüsselung nötig ist:

BETREIBER

Verschlüsselte Datenbank. Sacom EDV GmbH verwahrt die clientseitig verschlüsselte Datenbank. Ohne die zugehörigen Schlüssel ist sie nicht mehr als ein Block aus Bytes – mathematisch nicht von einer zufälligen Datei zu unterscheiden.

TREUHÄNDER

Situationsschlüssel. Ein Anwalt oder Notar, ausgewählt vom Ersteller, verwahrt den Situationsschlüssel. Er gibt ihn erst nach Prüfung des Ernstfalls an die Berechtigten weiter. Ohne Datenbank und ohne Benutzer-schlüssel ist er nutzlos.

BEGÜNSTIGTE:R

Benutzerschlüssel. Die vom Ersteller benannte Person erhält ihren Benutzerschlüssel vorab – physisch, z. B. als QR-Code im versiegelten Umschlag oder im Safe. Ohne Situationsschlüssel und ohne Datenbank kann man damit nichts anfangen.

Erst wenn alle drei Teile *beim Berechtigten* zusammenkommen – die Datenbank von Sacom, der Situationsschlüssel vom Treuhänder und der eigene Benutzerschlüssel – werden nur die für die Situation vorgesehenen Daten für die entsprechenden Berechtigten lesbar. Es gibt keinen Master-Schlüssel, der einen der drei Teile ersetzen könnte. Es gibt keine Recovery-Datenbank beim Betreiber, die zur Not eine zweite Tür aufstoßen würde. Es gibt keinen technischen Pfad, über den Sacom als Betreiber die Inhalte sehen oder rekonstruieren könnte – nicht zugunsten des Kunden, nicht zugunsten von Behörden, nicht zugunsten der Geschäftsleitung. Diese Aussage ist kein Versprechen, sondern eine Folge davon, dass die fehlenden Teile bei dem Betreiber *nicht existieren*.

Verschlüsselt wird einmal, geprüft wird mathematisch

Die Daten werden auf dem Gerät des Erstellers mit Post-Quantum-Algorithmen verschlüsselt. Was den Server verlässt, ist bereits Ciphertext. Niemand sieht den Klartext. Die übertragene Datenbank ist "eingefroren" und zustandslos aber mit den korrekten kryptographischen Schlüsseln in den jeweils vorgesehenen Teilen jederzeit lesbar.

> *Die Sicherheit sitzt nicht in der Logik-Regel, sondern in der mathematischen Struktur, die nicht mehr im Code und der Datenbank umkonfiguriert werden kann.*

Das ist der Unterschied zwischen einer Software, die sich entscheidet, nicht hinzusehen, und einer Software, die nicht hinsehen *kann*. Im ersten Fall ist Sicherheit eine Vertrauensleistung. Im zweiten Fall ist sie eine Eigenschaft der Konstruktion. Vertrauen lässt sich brechen. Eine Konstruktionseigenschaft nicht.

04 Das Patent – die unsichtbare Innovation

Worum es bei M.I.A. wirklich geht – und wo die Erfindung beginnt.

Hinweis: Das Verfahren wurde beim Europäischen Patentamt angemeldet, eine Erteilung liegt bislang nicht vor.

M.I.A. beschreibt eine Zugriffsarchitektur, in der die Frage „darf zugegriffen werden?“ vollständig durch die Frage "kann zugegriffen werden" ersetzt wird. Das Patent verschiebt den Ort der Sicherheit – weg von einer entscheidenden Software-Regel, hin zu einer Schlüssel-Konstellation, deren Erfüllbarkeit unabhängig vom laufenden Code ist. Es ersetzt eine bedingte Aussage durch eine geometrische.

Was das Patent *nicht* ist

- **Kein zweiter Faktor.** 2FA addiert eine Hürde zu einem bestehenden Login-Pfad. M.I.A. lehnt einen Login-Pfad als Konzept ab.
- **Kein Rollenmodell.** RBAC o.ä. weist Berechtigungen zu, die ein Admin verwaltet. M.I.A. kennt keinen Admin, der Berechtigungen verwalten könnte.
- **Kein Treuhand-Verfahren auf Vertrauensbasis.** Klassische Treuhand-Modelle laufen auf eine Stelle hinaus, die im Zweifel doch alles weiß. In M.I.A. weiß keine einzelne Stelle alles – auch nicht der Treuhänder selbst.

Was das Patent ist

Es ist die Beschreibung eines Verfahrens, in dem die wirtschaftliche und rechtliche Trennung der drei Parteien sich in der mathematischen Struktur des Schlüsselmaterials spiegelt. Die Beteiligten sind nicht durch eine Vereinbarung getrennt – sie sind durch die Konstruktion des Schlüssels selbst getrennt. Wer als Betreiber wissen will, was im Datenpaket steht, muss nicht eine Vereinbarung brechen. Er muss Mathematik brechen.

> Das Patent beschreibt kein zusätzliches Schloss, sondern eine jedes Mal individuell gebaute Tür, die durch die Schlüssel selbst definiert ist.

Wenn Sicherheit nicht mehr in einer Regel sitzt, sondern in der Form des Schlüssels, dann lässt sie sich nicht mehr durch ein Update verändern, nicht mehr durch eine Konfigurationsdatei aufweichen, nicht mehr durch einen falschen Klick eines Administrators verlieren. Die Eigenschaft hängt nicht mehr am Verhalten – sie hängt an der Form. Und Formen sind, anders als Verhaltensweisen, nicht verhandelbar.

05 Vergleichsmatrix – was emna ergänzt, was emna anders macht

Warum emna kein Ersatz für bestehende Instrumente ist – sondern die Schicht, die bisher gefehlt hat.

Testament, Vorsorgevollmacht, Patientenverfügung – all diese Instrumente existieren, und sie sind wichtig. emna ersetzt keines davon. Was emna macht: Es schließt die Lücken *in und zwischen* diesen Instrumenten.

INSTRUMENT	WAS ES LEISTET	WAS ES NICHT LEISTET
Testament	Regelt Vermögensnachfolge. Rechtlich bindend.	Wird *allen* Erben verlesen – keine individuellen Botschaften, keine vertraulichen Zugänge, kein situationsabhängiger Zugriff. Nur bei Tod.
Vorsorgevollmacht	Bestimmt, wer bei Handlungsunfähigkeit entscheidet.	Regelt *wer*, nicht *was*. Enthält keine Konten, keine Zugänge, keine Anweisungen, keine persönlichen Botschaften.
Patientenverfügung	Regelt medizinische Entscheidungen.	Sagt nichts darüber, wer sich um die Kinder kümmert, wo die Versicherung liegt oder welche Daueraufträge laufen.
Passwort-Manager	Speichert Zugänge zentral und sicher.	Kennt keine Situationen, keine unabhängige Prüfung, keine persönlichen Botschaften. Kein Schutz gegen Missbrauch durch Master-Passwort-Inhaber.
Plattform-Nachlass	Gibt Zugehörigen Zugriff auf ein einzelnes Konto.	Nur für die eigene Plattform, nur im Todesfall, keine situationsbasierte Steuerung, kein Überblick.
Zettel im Tresor	Sofort verfügbar, keine Technik nötig.	Veraltet sofort. Keine Situationssteuerung. Wer den Tresor öffnet, sieht alles – unabhängig davon, ob er alles sehen soll.

emna löst die Probleme der rechten Spalte: Es transportiert *persönliche Botschaften, Zugänge, Dokumente und Anweisungen* – vertraulich, situationsabhängig, individuell pro Berechtigtem. Nicht öffentlich wie ein Testament. Nicht auf eine Plattform begrenzt. Nicht veraltet wie ein Zettel. Und geschützt durch eine Architektur, bei der niemand allein öffnen kann – nicht einmal der Betreiber. Und bei korrekter Anwendung mit rechtlicher Bindungswirkung.

> emna ersetzt kein rechtliches Dokument. emna ergänzt, was kein rechtliches Dokument leisten kann.

Juristische Einbettung

emna kann in bestehende Rechtsinstrumente eingebunden werden – als Verweis, nicht als Ersatz. Ein eigenhändiges

Testament (§ 2247 BGB) darf auf emna als Aufbewahrungsort ergänzender Informationen verweisen, solange die testamentarischen Verfügungen selbst im Testament stehen. Die Vorsorgevollmacht kann emna als Quelle für Anweisungen im Innenverhältnis benennen (§§ 167, 665 BGB). Und bei der Patientenverfügung können in emna hinterlegte Wertvorstellungen als Erkenntnisquelle für den mutmaßlichen Willen dienen (§ 1827 Abs. 2 BGB).

Entscheidend: Gerichte sind bei der Testamentsauslegung verpflichtet, alle Umstände außerhalb der Urkunde heranzuziehen, um den wirklichen Willen des Erblassers zu erforschen (§§ 133, 2084 BGB – Andeutungstheorie). In emna hinterlegte Inhalte haben dabei eine höhere Beweisqualität als mündliche Äußerungen: schriftlich fixiert, zeitlich dokumentiert, durch das Drei-Parteien-Modell manipulationssicher.

06 Fallbeispiel – ein Vorsorge-Fall in 30 Sekunden

Zwei QR-Codes scannen. Alle Informationen verfügbar. Keep it simple and stupid.

Frau M. ist Mitte Dreißig, alleinerziehend, alleinige Sorgeberechtigte für ihre Tochter. Sie legt in emna im Voraus an, was im Notfall verfügbar sein soll: Allergien des Kindes, Notfallkontakte, eine schriftliche Botschaft, eine Liste der wichtigsten Konten, eine Handreichung für ihre Schwester über den Tagesablauf der Tochter, eine Vorsorgevollmacht. Sie wählt einen Anwalt aus dem Treuhänder-Kreis als Treuhänder und ihre Schwester als Begünstigte.

Was passiert in dem Moment, in dem das Unvorhersehbare eintritt?

Frau M. hat ihrer Schwester vorab einen versiegelten Umschlag mit dem Benutzerschlüssel übergeben – für den Fall der Fälle. Die Schwester weiß, dass der Umschlag existiert, aber nicht, was in der Datenbank steht.

VORSORGEFALL — SCHEMATISCH

1. Frau M. ist nach einem Unfall handlungsunfähig. Die Schwester benachrichtigt den Treuhänder, legt das ärztliche Attest vor.
2. Der Treuhänder prüft den Nachweis nach dem im ICE-Protokoll definierten Katalog. Er handelt als Anwalt mit beruflicher Haftung – keine Software ersetzt diese Prüfung.
3. Bei positiver Prüfung gibt der Treuhänder den *Situationsschlüssel* an die Schwester frei und sendet eine signierte Freigabeanweisung an die Sacom.
4. Sacom überträgt die verschlüsselte Datenbank an die Schwester. Erst jetzt hat sie alle drei Teile: ihren Benutzerschlüssel aus dem Umschlag, den Situationsschlüssel vom Treuhänder und die Datenbank von Sacom. Erst jetzt entsteht aus den Bytes wieder lesbarer Inhalt.
5. In der Anzeige für die Schwester steht, was sie braucht: die Allergien des Kindes, der Tagesablauf, die Botschaften, die Konten. Nicht mehr. Nicht weniger.

Aus Sicht der Beteiligten passiert nichts Aufregendes. Es gibt kein Diagramm, das Schlüsselteile als animierte Funken zeigt. Kein Dashboard, das mit Fortschrittsbalken zur Erfüllung läuft. Die Eleganz liegt in der Einfachheit. Keep it simple and stupid (K.I.S.S.). Die UI zeigt nur das an, was lesbar ist. Mehr Informationen gibt es nicht. Auch kein "Access denied to 'Banking PIN'".

Aus Sicht der Architektur passiert genau das, was passieren soll: drei Teile finden in der richtigen Reihenfolge zusammen, und ein zuvor unlesbarer Datenblock wird zu einer geordneten, strukturierten, verständlichen Hilfe für eine Familie in einer schwierigen Situation. Die Komplexität bleibt unter der Haube. Sie interessiert den Benutzer nicht.

07 Fazit

emna und M.I.A. - Jeweils selbstständig und gemeinsam hervorstehend stark

Vorsorge besteht heute aus Inseln. Das Testament regelt das Erbe, die Vollmacht regelt die Vertretung, die Patientenverfügung regelt die Medizin. Aber zwischen diesen Inseln liegt ein Ozean aus ungeregelten Fragen: Wer kümmert sich um die Kinder? Wo liegt die Versicherung? Was soll mein Partner wissen – und was erst nach meinem Tod? Welche Botschaft soll bleiben?

emna schließt diese Lücken. Nicht als Ersatz für rechtliche Dokumente, sondern als die Schicht, die bisher fehlte: persönliche Botschaften, Zugänge, Dokumente und Anweisungen – vertraulich, situationsabhängig, individuell pro Berechtigtem. Juristisch einbettbar in Testament, Vorsorgevollmacht und Patientenverfügung. Geschützt durch eine Architektur, bei der nicht einmal der Betreiber lesen kann, was verwahrt wird.

Denn das ist der eigentliche Punkt: Die Vertrauenswürdigkeit des Betreibers ist fast irrelevant geworden. Nicht weil Sacom sich entschieden hat, nicht hinzusehen – sondern weil das Hinsehen außerhalb ihrer Möglichkeit liegt. Das ist kein Versprechen. Das ist eine Konstruktionseigenschaft.

> emna ist das Gespräch, das bleibt – auch wenn man selbst nicht mehr sprechen kann.

Eine Anwendung, die im Alltag fast unsichtbar ist und sich erst im Ernstfall in ihrer Bedeutung zeigt. So einfach wie einen Brief zu schreiben. So sicher wie Mathematik es erlaubt. Und so menschlich wie das Gespräch, das dahintersteht.

M.I.A. – über emna hinaus

emna ist die Referenzimplementierung von M.I.A. – aber nicht die einzig denkbare. Das Prinzip, Zugriff nicht durch Software-Regeln, sondern durch mathematische Schlüsselkonstellationen zu steuern, lässt sich auf jedes Szenario übertragen, in dem sensible Informationen erst unter definierten Bedingungen und nur für bestimmte Empfänger zugänglich werden sollen:

- **Journalismus & Whistleblowing** – Hinweise, die erst bei Eintritt einer definierten Situation entschlüsselbar werden
- **Militär und Nachrichtendienste** – situationsabhängige Freigabe von Einsatzinformationen ohne zentrale Schwachstelle
- **Banken und Finanzwesen** – Treuhandkonstellationen, bei denen kein einzelner Beteiligter einseitig verfügen kann
- **Unternehmensnachfolge** – Betriebsgeheimnisse, die im Erbfall gezielt an einzelne Nachfolger gehen

Überall dort, wo heute Vertrauen in eine zentrale Stelle nötig ist, kann M.I.A. dieses Vertrauen durch eine unveränderliche Konstruktionseigenschaft ersetzen. emna zeigt, wie das in der Praxis aussieht – für den Bereich, der jeden Menschen betrifft: die Vorsorge für den Ernstfall.

Über emna. emna ist eine digitale Vorsorge-Plattform der Sacom EDV GmbH mit der zum Patent angemeldeten Zugriffsarchitektur M.I.A. (Mathematical Immutable Access). Die Plattform richtet sich an Familien, Unternehmer, alleinerziehende Eltern und Personen mit erhöhtem Vertraulichkeitsbedarf. Mehr unter **emna.app**.

Dieses Whitepaper beschreibt das Verfahren auf konzeptioneller Ebene. Implementierungsdetails unterliegen dem laufenden Patent-Verfahren und werden nach dessen Abschluss vollständig dokumentiert.