

# Serverless and databaseless encryption technology

## Technologie de chiffrement sans serveur ni base de données

### 5. Development potential of DataShielder Suite

The upcoming integration of Freemindtronic's EviDNA technology into the DataShielder Suite is based on the advanced use of DNA sequencing to create unique secret keys, each protected by robust security measures. This technology employs the DNA sequencing of a human being, consisting of over 600,000 lines of sequences, each line containing 20 sequencing codes, thus totaling 12,000,000 sequencing codes per individual. This exceptional granularity enables extremely precise identification of individuals, including the ability to distinguish between twins, and even between dizygotic twins through precision adjustments. This ensures that each secret key generated by the EviDNA technology is unique for each individual.

This identification capability is particularly crucial in military applications, such as the rapid and reliable identification of fallen soldiers or the authentication of physically unknown individuals in operational theaters.

EviDNA technology, integrated into DataShielder Defense within the DataShielder Suite, will primarily serve sovereign entities, offering high levels of authentication and data security. Its scope is not limited to the military domain; it extends to sectors requiring rigorous authentication and data security, such as the security of critical infrastructures and medical applications, where the precision of genetic data is crucial. The adaptability and accuracy of EviDNA technology promise to broaden its impact, thus enhancing its strategic value for both civilian and military uses, ensuring robust protection in various operational environments.

Use Cases:

#### **Post-Mortem Identification:**

In the military context, EviDNA enables rapid and reliable identification of fallen soldiers through a public key tattoo based on their DNA. This tattoo, applied by flocking with a durable dye visible or invisible, can be directly placed on the skin or personal belongings of soldiers. These keys, generated from the soldier's DNA and compacted for inclusion in QR codes, provide a durable and extreme condition-resistant method of identification. This solution, both economical and effective, ensures persistent identification, suitable even long after in challenging operational environments.

#### **Communications Security:**

EviDNA will enhance the security of strategic communications by generating unique keys for each identified user, enabling the encryption of exchanges between units in the field. This system will ensure that only authorized parties, previously authenticated by a DNA-based identification process, can access encrypted information. The use of EviDNA in the EviCypher encryption technology, integrated into DataShielder products, provides advanced cryptographic key management. This includes securing files and messaging

communications while effectively preventing identity theft. This approach significantly strengthens the confidentiality and security of military and strategic communications, ensuring user identities are verified before any access to secured data.

#### **Secure Access Control:**

The access control system to sensitive infrastructures will integrate EviDNA to enhance security and specificity of access. Using DNA-based keys from pre-analyzed sequences, EviDNA will enable fail-proof authentication, effectively preventing unauthorized access to critical areas or information. These segmented keys increase security by ensuring precise access verification. Advantageously, EviDNA will also be implemented with a patent on wireless access control, already integrated into the DataShielder NFC HSM solution, further strengthening protection mechanisms in applications where security is paramount.

#### **Security Protocol Development:**

EviDNA is likely to play a central role in developing new biometric security protocols for military and governmental applications. By incorporating genetic data, EviDNA strengthens authentication mechanisms, allowing the development of advanced security protocols that use these precise data to secure critical environments. This approach will substantially improve the integrity and reliability of security processes, making genetics a fundamental pillar of modern authentication systems.

#### **Identity Management:**

We are confident that in the short term, we can integrate EviDNA into our Cardokey Pro Badge products, particularly to create military access badges. These devices already use cryptographic keys, but with the introduction of DNA as the basis of authentication, we will provide an additional level of security. Through the integration of EviDNA and segmented key authentication, these identification devices will offer enhanced security, becoming tamper-proof and highly personalized. This evolution will increase the reliability of identification systems within the armed forces, especially in operational theaters. The cards will only be decipherable by authorized systems, operating offline without the need for a server or database. Adopting EviDNA in these military identity cards will ensure that each identification is not only secure but also specifically tailored to each user, thus consolidating the protection of personal and operational information.

#### **Data Integrity and Verification:**

In the future, data integrity and the verification of military documents and orders will be assured by using EviDNA digital signatures. These signatures will confirm the authenticity and integrity of strategic documents and orders, ensuring the data remains secure and authentic. Freemindtronic's EviSign technology, to be presented for the first time at Eurosatory 2024 and integrated into the DataShielder HSM PGP solution, will allow the signing of sensitive data without a server or database. The signature keys, freely generated by the user without reliance on a third party, will validate that the documents have not been altered and come from a reliable source, thereby enhancing the security of military operations and critical infrastructures.

### **8. Contribution of DataShielder NFC HSM to the Energy Transition**

**Energy Efficiency:** DataShielder NFC HSM stands out for its on-demand operation, consuming energy only when activated, eliminating any standby energy consumption. This feature significantly reduces the energy footprint, aligning our technology with the goals of the energy transition.

**Cybersecurity Innovation:** Our suite has been recognized for its innovative approach to cybersecurity, earning us the Fortress 2023 Cyber Security Award. By securing data efficiently and economically, we contribute to a greener digital infrastructure.

**Serverless and Databaseless Solution:** As a solution that requires neither servers nor databases, DataShielder NFC HSM reduces reliance on energy-intensive data centers, thus promoting more responsible use of computing resources.

**Versatility and Adaptability:** Our suite’s EviCore HSM OpenPGP technology enables the transformation of various supports into hardware security modules (HSM), enhancing the flexibility and energy efficiency of our solutions.

**Support for Legal Standards:** With integrated EviSign technology, we enable electronic document signing with legally recognized value, ensuring the integrity and authenticity of the data.

**Dual-Use for Civilian and Military Applications:** Our Dual-Use version, suitable for both civilian and military applications, provides an appropriate level of protection for each context, contributing to better energy resource management across various sectors.

**Data Durability:** Data stored in DataShielder’s NFC memory is estimated to last 60 years without the need for energy, and the memory can be rewritten up to 1 million times without risk of error. This ensures exceptional longevity and unprecedented reliability, reducing the need for frequent maintenance and replacement.

**Environmental Commitment:** We are determined to reduce our carbon footprint. Our components made of PCB FR4 170, without plastic, connectors, keyboards, or screens, are designed for high durability and longevity, thus minimizing waste and the energy required to produce new hardware.

===== Traduction française =====

**5. Votre potentiel d'évolution**

La prochaine intégration de la technologie EviDNA de Freemindtronic dans DataShielder Suite repose sur l'utilisation avancée du séquençage de l'ADN pour créer des clés secrètes uniques, chacune protégée par des mesures de sécurité robustes. Cette technologie utilise le séquençage de l'ADN d'un être humain composé de donnée séquençage de plus de 600,000 lignes de séquences, avec chaque ligne contenant 20 codes de séquençage, totalisant ainsi 12,000,000 de codes de séquençage par individu. Cette granularité exceptionnelle permet l'identification extrêmement précise d'individus, y compris la capacité de distinguer entre des jumeaux, et même entre des

jumeaux dizygotes par des ajustements de précision. Ce qui garantit que chaque clé secrète générée par la technologie EviDNA est unique pour chaque individu. Cette capacité d'identification est particulièrement cruciale dans des applications militaires, comme l'identification rapide et fiable de soldats tombés au combat ou l'authentification des personnes physiquement inconnues sur théâtre d'opérations. La technologie EviDNA, intégrée dans DataShielder Defense de la suite DataShielder, sera principalement dédiée aux entités régaliennes, offrant des niveaux élevés d'authentification et de sécurisation des données. Sa portée ne se limite pas au domaine militaire ; elle s'étend à des secteurs nécessitant une authentification poussée et une sécurisation des données, comme la sécurité des infrastructures critiques et les applications médicales, où la précision des données génétiques est cruciale. La capacité d'adaptation et la précision de la technologie EviDNA promettent d'élargir son impact, augmentant ainsi sa valeur stratégique pour les utilisations tant civiles que militaires, garantissant une protection robuste dans divers environnements opérationnels.

### **Cas d'usage :**

#### **Identification post-mortem :**

Dans le contexte militaire, EviDNA permet une identification rapide et fiable des soldats tombés au combat grâce à un tatouage de clés publiques basé sur leur ADN. Ce tatouage, appliqué par flocage avec une teinture durable visible ou invisible, peut être directement apposé sur la peau ou les effets personnels des soldats. Ces clés, générées à partir de l'ADN du soldat et compactées pour inclusion dans des QR codes, offrent une méthode d'identification durable et résistante aux conditions extrêmes. Cette solution, à la fois économique et efficace, assure une identification persistante, adaptée même longtemps après dans des environnements opérationnels difficiles.

#### **Sécurité des Communications :**

EviDNA renforcera la sécurité des communications stratégiques en générant des clés uniques pour chaque utilisateur identifié, permettant de crypter les échanges entre les unités sur le terrain. Ce système garantira que seules les parties autorisées, préalablement authentifiées par un processus d'identification basé sur l'ADN, puissent accéder aux informations chiffrées. L'utilisation d'EviDNA dans la technologie de chiffrement EviCypher, intégrée aux produits DataShielder, assure une gestion avancée des clés cryptographiques. Cela inclut la sécurisation des fichiers et des communications de messagerie, tout en prévenant efficacement l'usurpation d'identités. Cette approche renforce considérablement la confidentialité et la sécurité des communications militaires et stratégiques, garantissant que l'identité des utilisateurs est vérifiée avant tout accès aux données sécurisées.

#### **Contrôle d'Accès Sécurisé :**

Le système de contrôle d'accès aux infrastructures sensibles intégrera EviDNA pour renforcer la sécurité et la spécificité des accès. Utilisant des clés basées sur l'ADN issues de séquences pré-analysées, EviDNA permettra une authentification infaillible, empêchant efficacement les accès non autorisés à des zones ou informations critiques. Ces clés segmentées augmentent la sécurité en assurant une vérification d'accès précise. Avantagusement, EviDNA sera également implémenté avec une mise en œuvre du brevet sur le contrôle d'accès sans fil, déjà intégré dans la solution DataShielder NFC

HSM, renforçant ainsi les mécanismes de protection dans les applications où la sécurité est primordiale.

### **Développement de Protocoles de Sécurité :**

EviDNA est susceptible de jouer un rôle central dans le développement de nouveaux protocoles de sécurité biométriques pour les applications militaires et gouvernementales. En intégrant les données génétiques, EviDNA renforce les mécanismes d'authentification, permettant l'élaboration de protocoles de sécurité avancés qui utilisent ces informations précises pour sécuriser les environnements critiques. Cette approche améliorera substantiellement l'intégrité et la fiabilité des processus de sécurité, en faisant de la génétique un pilier fondamental des systèmes d'authentification modernes.

### **Gestion de l'Identité :**

Nous envisageons avec certitude qu'à court terme, nous pourrions intégrer EviDNA dans nos produits Cardokey Pro Badge, notamment pour créer des badges d'accès militaires. Ces dispositifs utilisent déjà des clés cryptographiques, mais avec l'introduction de l'ADN comme base de l'authentification, nous apporterons un niveau de sécurité supplémentaire. Grâce à l'intégration de la technologie EviDNA et de l'authentification à clé segmentée, ces dispositifs d'identification offriront une sécurité renforcée, devenant infalsifiables et hautement personnalisés. Cette évolution augmentera la fiabilité des systèmes d'identification au sein des forces armées, particulièrement en théâtre d'opération. Les cartes seront déchiffrables uniquement par des systèmes autorisés, fonctionnant hors ligne sans nécessiter de serveur ni de base de données. L'adoption d'EviDNA dans ces cartes d'identité militaires garantira que chaque identification est non seulement sécurisée mais également spécifiquement adaptée à chaque utilisateur, consolidant ainsi la protection des informations personnelles et opérationnelles.

### **Intégrité des Données et Vérification :**

On peut imaginer qu'à l'avenir, l'intégrité des données et la vérification des documents et commandes militaires seront assurées par l'utilisation des signatures numériques EviDNA. Ces signatures confirmeront l'authenticité et l'intégrité des documents et commandes stratégiques, garantissant que les données restent sécurisées et authentiques. La technologie EviSign de Freemindtronic, qui sera présentée pour la première fois à Eurosatory 2024 et intégrée dans la solution DataShielder HSM PGP, permettra de signer des données sensibles sans serveur ni base de données. Les clés de signature, générées librement par l'utilisateur, sans recours à un tiers de confiance, valideront que les documents n'ont pas été modifiés et qu'ils proviennent d'une source fiable, renforçant ainsi la sécurité des opérations militaires et des infrastructures critiques.

## **8. Contribution de DataShielder NFC HSM à la Transition Énergétique**

**Efficacité Énergétique :** DataShielder NFC HSM se distingue par son fonctionnement à la demande, sans consommation d'énergie en veille. Cette caractéristique assure une réduction significative de l'empreinte énergétique, alignant notre technologie avec les objectifs de la transition énergétique.

**Innovation en Cybersécurité** : Notre suite a été reconnue pour son approche innovante en matière de cybersécurité, ce qui nous a valu le prix Fortress 2023 Cyber Security Award. En sécurisant les données de manière efficace et économe, nous contribuons à une infrastructure numérique plus verte.

**Solution sans Serveur ni Base de Données** : la dépendance aux centres de données énergivores est réduite, favorisant ainsi une utilisation plus responsable des ressources informatiques.

**Polyvalence et Adaptabilité** : La technologie EviCore HSM OpenPGP de notre suite permet de transformer divers supports en modules de sécurité matériels (HSM), renforçant la flexibilité et l'efficacité énergétique de nos solutions.

**Soutien aux Normes Légales** : Grâce à la technologie EviSign intégrée, nous permettons la signature électronique de documents avec une valeur juridiquement reconnue, tout en garantissant l'intégrité et l'authenticité des données.

**Notre version Double Usage** offre un niveau de protection adapté à chaque contexte, contribuant ainsi à une meilleure gestion des ressources énergétiques dans divers secteurs.

**Durabilité des Données** : Les données stockées dans la mémoire NFC de DataShielder sont estimées à 60 ans sans avoir besoin d'énergie, et la mémoire peut être réécrite jusqu'à 1 million de fois sans risque d'erreur. Cela garantit une longévité exceptionnelle et une fiabilité sans précédent, réduisant le besoin de maintenance et de remplacement fréquent.

**Engagement Environnemental** : Nous sommes déterminés à réduire notre empreinte carbone. Nos composants en PCB FR4 170, sans plastique, connecteurs, claviers ou écrans, sont conçus pour une grande durabilité et longévité, minimisant ainsi les déchets et l'énergie nécessaire à la production de matériel neuf.