

KEY CUSTODY CONTINUITY

For the keys you can never lose.

An extra layer beneath the protection you already have.

DNA Shield keeps one share of your most important keys, and the instructions to rebuild them, offline in DNA for decades.

WHY THIS MATTERS

Every certificate, login and signed payment depends on a few root keys. Large organizations protect them well, with HSM clusters across sites, smartcards in safes, vendor backup and rehearsed ceremonies. That covers hardware failure, losing a site and losing one key holder. But some keys are used rarely and must last for decades: offline roots, firmware-signing roots, archive keys and new post-quantum roots.

SOME RISKS MAY REMAIN

Everything failing together

Every copy sits inside the same estate, vendor or identity system.

Decades passing

People, suppliers and formats change faster than root keys.

Vendor end-of-life

Backups locked to hardware that may not exist in 20 years.

WHAT DNA SHIELD DOES

DNA Shield adds one extra share to your key scheme. It is written once into DNA, together with the instructions to use it, and kept outside your systems. Your scheme stays under your control, and Biomemory never holds a complete key. Recovery takes time. It is not instant. For keys you rarely use but can never lose, that does not matter.



Key holder A
PART 1



HSM site 1
PART 2



Key holder B
PART 3



HSM site 2
PART 4



DNA Shield
IN DNA

Your key in five parts, any three can rebuild it. DNA Shield holds one part, offline in DNA.

WHAT WE PROTECT

- Offline root CA keys
- Keys that decrypt long-term archives
- The instructions to rebuild them
- Firmware-signing root keys
- New post-quantum root keys
- The list of key holders

2 to 64 KB
typical size per key

Air-gapped
offline by design

Written once
no remote changes

0
energy used at rest

HOW IT WORKS FOR YOU

1

Choose

Pick an upcoming root, rollover or post-quantum migration.

2

Add a share

Split the key with one extra share. You encrypt it.

3

Store in DNA

Written once, sealed and kept offline in a vault.

4

Ask

An approved person asks in the portal. Every request is recorded.

5

Rebuild

We read it back. Your key holders rebuild the key in your HSM.

WHAT CHANGES

	Today	With DNA Shield
Where the backup is	On your network, or in your building	Offline, in a vault
If an admin password is stolen	It may reach everything, backups too	Nothing to log in to
How long it lasts	3 to 30 years, then copy again	Decades, even centuries
When people leave	Fewer key holders remain over time	The share and its instructions stay

NO NEW DEPENDENCY Your recovery still works without DNA Shield. Biomemory will hold the codec in escrow, so your data can be decoded even if Biomemory no longer exists, and will follow the SNIA DNA Data Storage Alliance standards.

WHO IT IS FOR

Device and IoT makers

Trust service providers

Organizations new to NIS2

Mid-sized banks and payments

Post-quantum migrations

Long-term archive owners

Usually led by the Head of PKI or Key Management, with the CISO.

THE RULES THAT ALREADY ASK FOR THIS

 **NIST SP 800-57** key backup

 **FIPS 140-3** keys stay in your HSMs

 **DORA, Article 12** separate backups

 **NIS2, Article 21** backup and recovery

 **eIDAS 2** secure signing keys

 **PCI DSS v4.0** split knowledge

DNA Shield supports these controls. It does not by itself make an organization compliant.

Let's protect the keys that matter most.

Start with an early access pilot at your next key ceremony: one key, one DNA share and one recovery test.

protectwithdna@biomemory.com | biomemory.com | Paris, Boston

AIR-GAPPED | BIOSECURE | IMMUTABLE | 150-YEAR MOLECULAR RETENTION