Encrypted Cloud Storage &
Blockchain Timestamping
Gee-nodes on Geens.com

www.geens.com

Geens.com =
You do have different “hats” in life - a Reputation System

1) Geens vault - pod (decentralised thinking = be empowered)

= private data, digital ID, logins and interests

= KYC, lifetime membership, NPO goes over generations

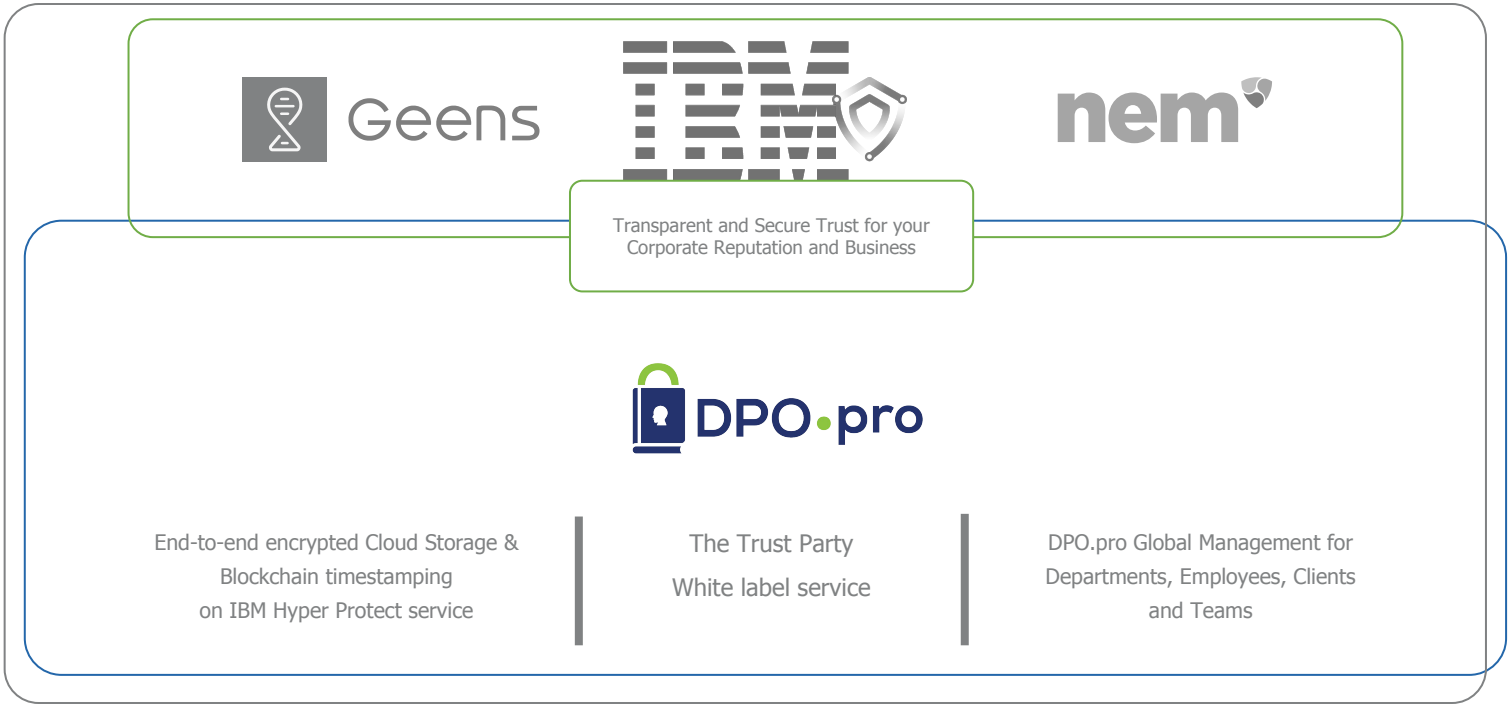
= trust, reputation, digital me

2) Geens for Business = cooperation platform (projects, businesses,...)

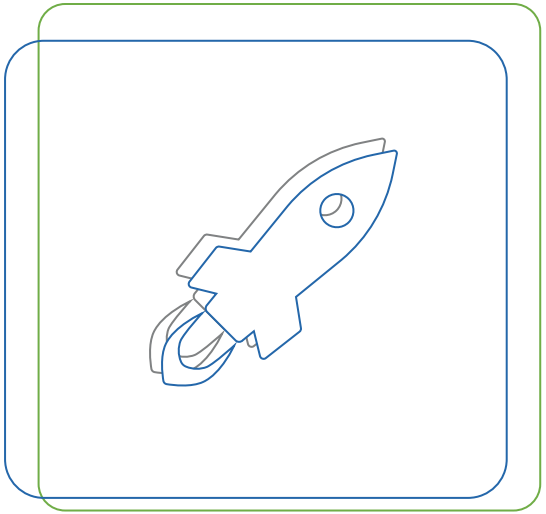
3) Gee-nodes = delegated trust given to “large” organisations (Identity Custodians)

= data sharing, recovery, environment, liability, gdpr, identity,...

Encrypted Cloud Storage & Blockchain Timestamping
Gee-nodes



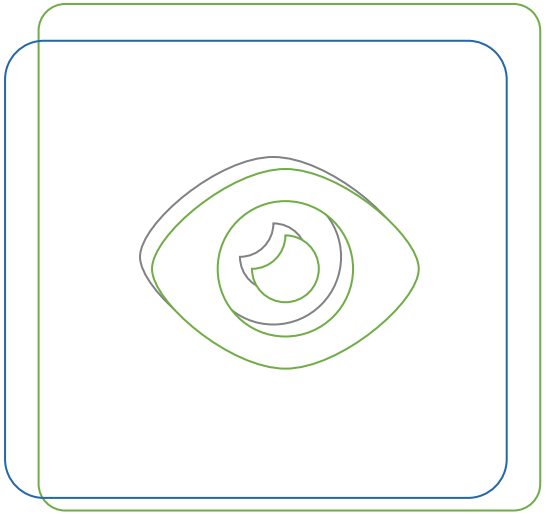
Encrypted Cloud Storage & Blockchain Timestamping
White label service



Mission:

Provide transparent, private and secure by design tools that are GDPR compliant to minimize risk and cost for personal data handling, businesses and professionals. Easy to use and integrated IOT solution with added value of services, micropayments and third party involvement.

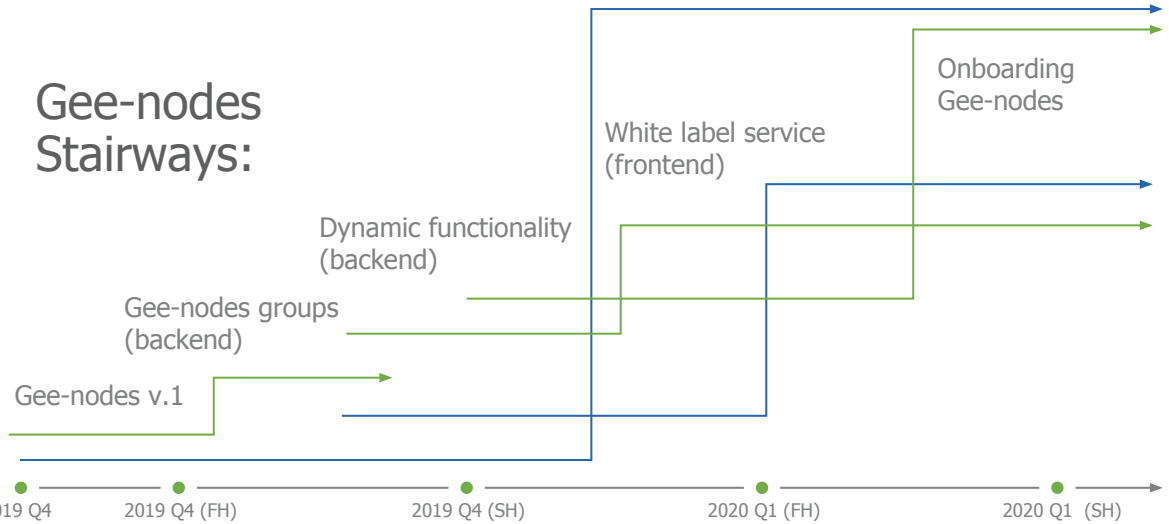
Encrypted Cloud Storage & Blockchain Timestamping
White label service



Vision:

Geens NPO is a non-governmental, non-profit, non-corporate organization which can never be owned or sold. Owned by the community and supervised by an Ethical Committee, the organisation assures data protection and anonymity.

Encrypted Cloud Storage & Blockchain Timestamping
Gee-nodes



Encrypted Cloud Storage & Blockchain Timestamping
White label service

Benefits:

1 Geens NPO
End-to-end encryption

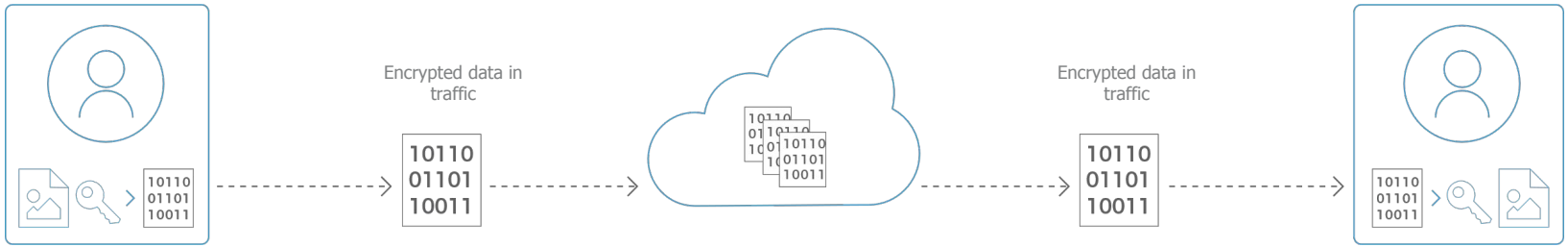
2 IBM
Hyper Protect

3 NEM.io
Blockchain

Encrypted Cloud Storage & Blockchain Timestamping
White label service

Geens NPO End-to-end encryption

By using end-to-end encryption, neither cloud providers nor system administrators can access encryption keys. The keys and user data are encrypted and stored on a server side only. Thereby, end-to-end encrypted cloud storage providers, such as Geens, can never access or decrypt users' data. If data breach happens on a server side, to identify encrypted users' data is impossible. Only encrypted data sets can be leaked. The content itself - as the most vulnerable data part - stays encrypted so no one can read it. Thus, your company's personal data and your clients' data will stay safe and private.



User A data is encrypted before leaving device

Cloud stores encrypted data therefore no one can access it

User B decrypts data on his device

Encrypted Cloud Storage & Blockchain Timestamping
White label service

IBM Hyper Protect

Hyper protect line of virtual servers service leverage the unparalleled security and reliability of Secure Service Containers on IBM Z/LinuxOne.

Hyper Protect Virtual Servers make it possible to bring IBM Z/LinuxOne into IBM's global public cloud data centers. Through the IBM Cloud catalog, you can gain easy access to industry-leading security capabilities to modernize your applications in the IBM Cloud.

Ability to deploy a Virtual Server in a Secure Service Container ensuring confidentiality of data and code running within the VS

Ability to deploy workload into the most secure, highly performant, Linux virtual server with extreme vertical scale

Run both core and non-core workloads in a public cloud, observing all security and compliance policies of your enterprise.

You can protect the assets of business while you simultaneously maintain enhanced business service levels.

You can instantiate Linux virtual servers with your own public SSH key. Thus, only you can access your code and data. Not even an IBM Cloud administrator has access to your data.

You can deploy any supported workload into the most secure, highly performant Linux system, taking advantage of strengths of the LinuxONE system.

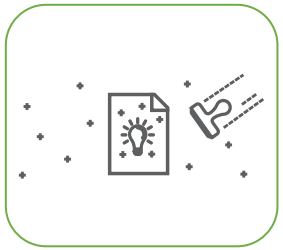
Encrypted Cloud Storage & Blockchain Timestamping
White label service

NEM.io Blockchain

Geens NPO in partnership with NEM foundation aims to empower people to securely access services of growing digital economy.

NEM Blockchain technology has the potential to change the way every industry manages its information and data. The Foundation details the opportunities in every industry to effectively store transaction, customer, and supplier data in a transparent, immutable ledger.

Automatic timestamping of signatures for registered mails



Protect ideas and content for patents

Protect copyrights: audio, visual, textual and other authentic work

Create a proof that you have been in a specific place at a specific time

Prove that the document was signed prior to a specific date

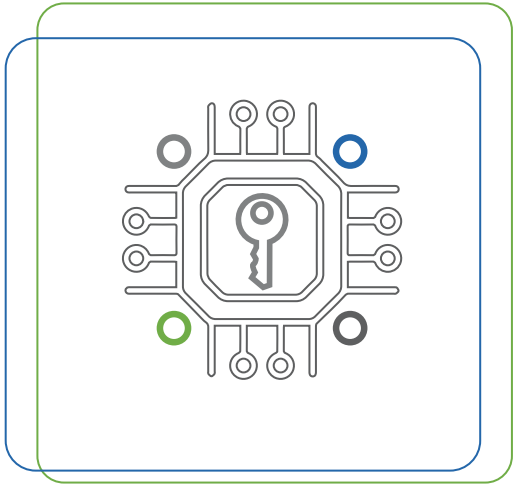
Encrypted Cloud Storage & Blockchain Timestamping

White label service

GDPR compliance:

GDPR compliant tools with End-to-end encryption service hosted on trusted cloud environment with an extra layer of security to share, manage, store data that can be accessed anytime on any device for the worldwide teams. Data management, client management, with privacy by design solutions.

Encrypted Cloud Storage & Blockchain Timestamping
White label service



How does end-to-end encryption help meet GDPR requirements?

Using cloud is less risky with encryption

Using cloud-based applications is convenient and efficient in your business, on the other hand, they could create risk or breaches of your data. To comply with GDPR, your organization as a data collector or forwarder is responsible for protecting the data during data assessment and management on your cloud based services.

General data protection regulation distinguishes encryption as one of the best ways to ensure data protection within your organization.

Encrypted Cloud Storage & Blockchain Timestamping
White label service

How does end-to-end encryption help meet GDPR requirements?

Article 32. Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a)the pseudonymization and encryption of personal data;

Encrypted Cloud Storage & Blockchain Timestamping
White label service

"In order to safeguard the security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design."

Marju Lauristin, Member of the European Parliament

How does end-to-end encryption help meet GDPR requirements?

Article 32. Security of processing

2. Use encryption to keep your data safe and secure from third party access.

There is always a possibility of data leakage or breach especially when dealing with third parties. End-to-end encryption assures that leaked data or data sets will stay unidentified. However, always keep in mind that "a confidentiality breach of personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified" to relevant supervisory authorities (WP29 Opinion 03/2014).

Encrypted Cloud Storage & Blockchain Timestamping
White label service

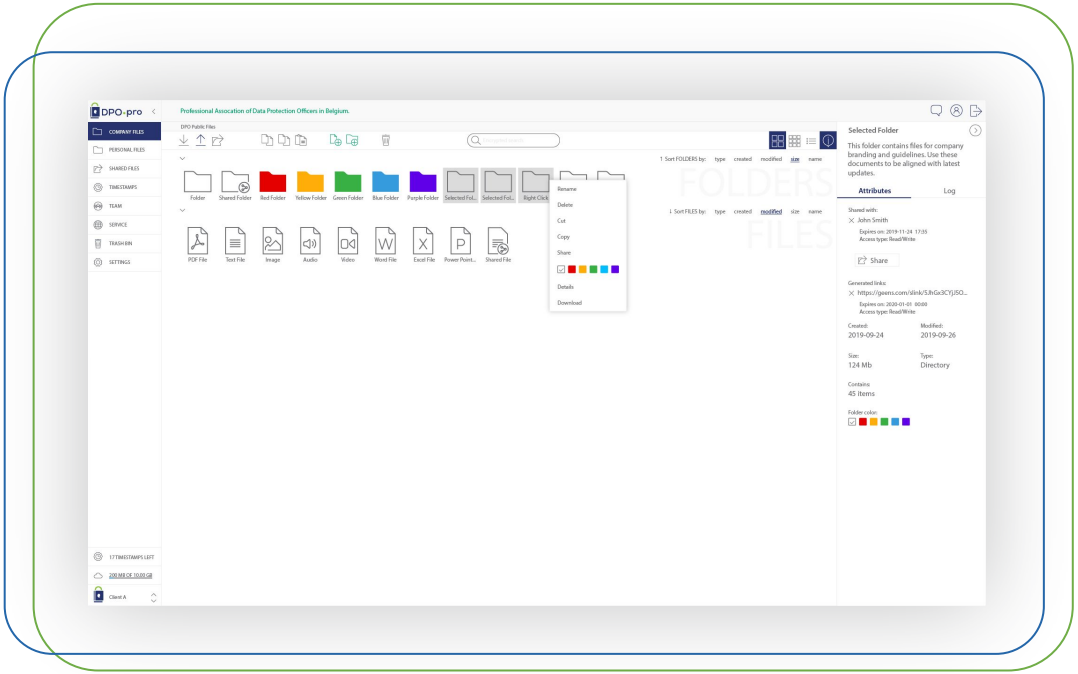
How does end-to-end encryption help meet GDPR requirements?

Article 32. Security of processing

3. End-to-end encryption is the way to go.

The GDPR will not specify or suggest what type of applications and their algorithms will thoroughly comply. Therefore, to ensure identification of a person or leaked data sets reidentification, encryption keys' management is crucial. By using end-to-end encryption with the client side key management, will hold a significantly stronger protection of private data.

Encrypted Cloud Storage & Blockchain Timestamping
White label service

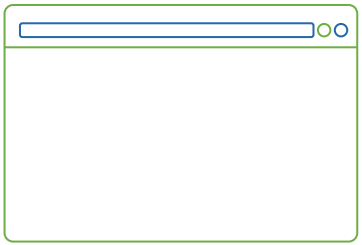


Advantages:

- White label
- Client Groups (nodes and sub-nodes)
- Roles, Assignment, Permissions
- GDPR compliant
- Data Blockchain Timestamping
- Activity logs (BC Timestamping for proof of existence and audit)

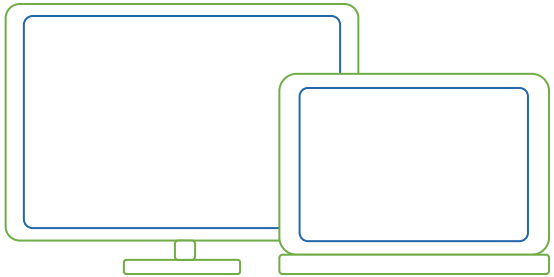
Encrypted Cloud Storage & Blockchain Timestamping
White label service

Tools:



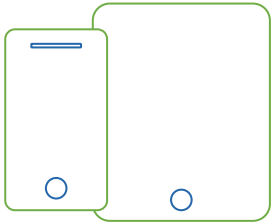
Web Application

Access from any device with browser.



Desktop Application

Cloud sync, access and work with native desktop apps.

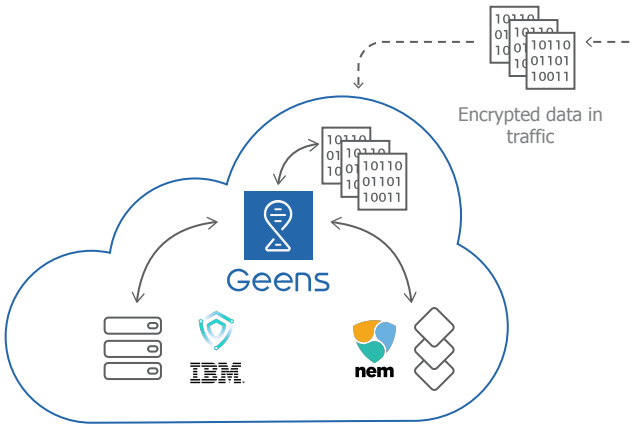


Mobile Application

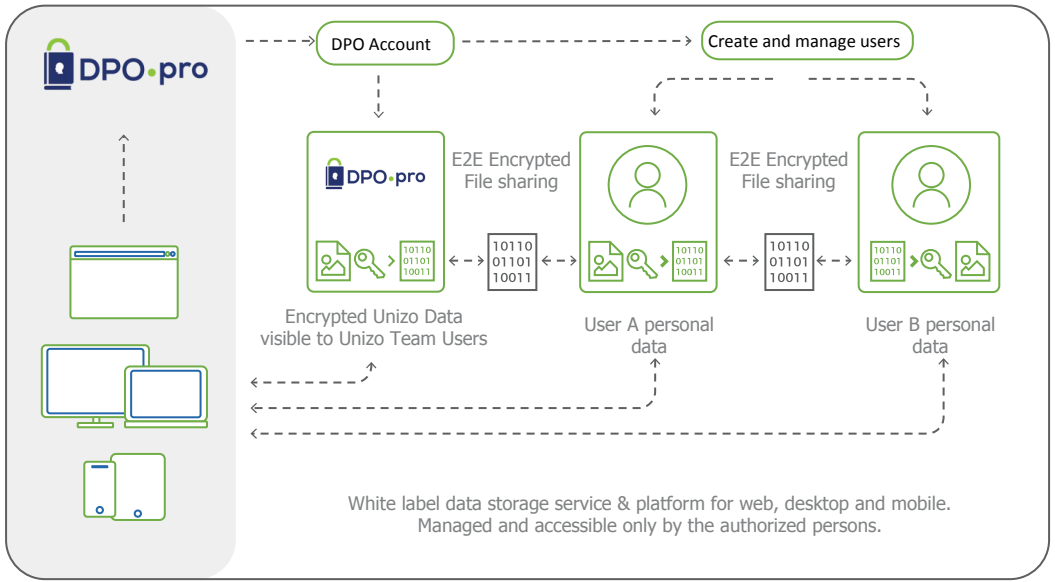
Access and work on the go, encrypted vault.

Encrypted Cloud Storage & Blockchain Timestamping
White label service

How It Works



Encrypted Cloud Storage that can be accessed only by users, running on IBM Hyperprotect servers and timestamped in blockchain for proof.

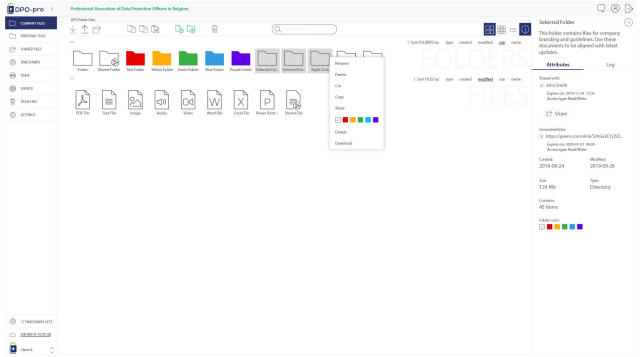


White label data storage service & platform for web, desktop and mobile.
Managed and accessible only by the authorized persons.

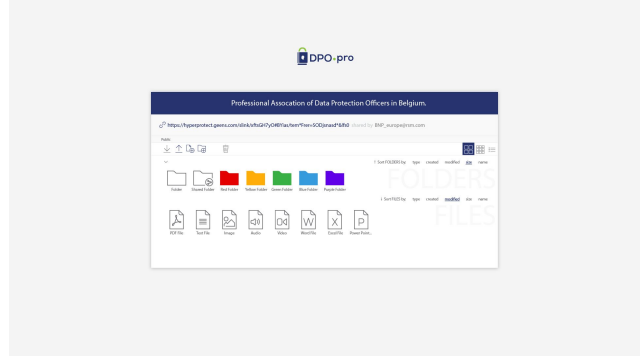
Encrypted Cloud Storage & Blockchain Timestamping
White label service

User interface

Log in Screen



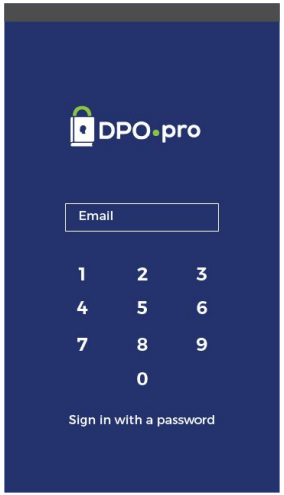
Application UI

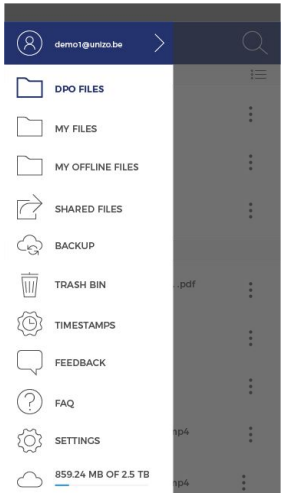


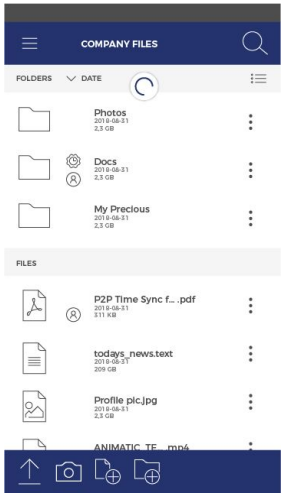
Public Share

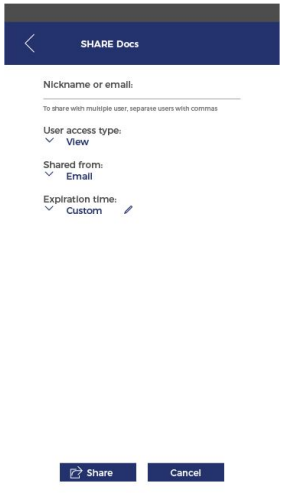
Encrypted Cloud Storage & Blockchain Timestamping
White label service

Mobile App









Encrypted Cloud Storage & Blockchain Timestamping
White label service

Use cases

Audit & assurance
After receiving a shared folder from Washington D.C. USA, gather evidence from the client who is anywhere from Africa to Asia and EU`s attorneys can immediately see a new evidence was added to the case folder.

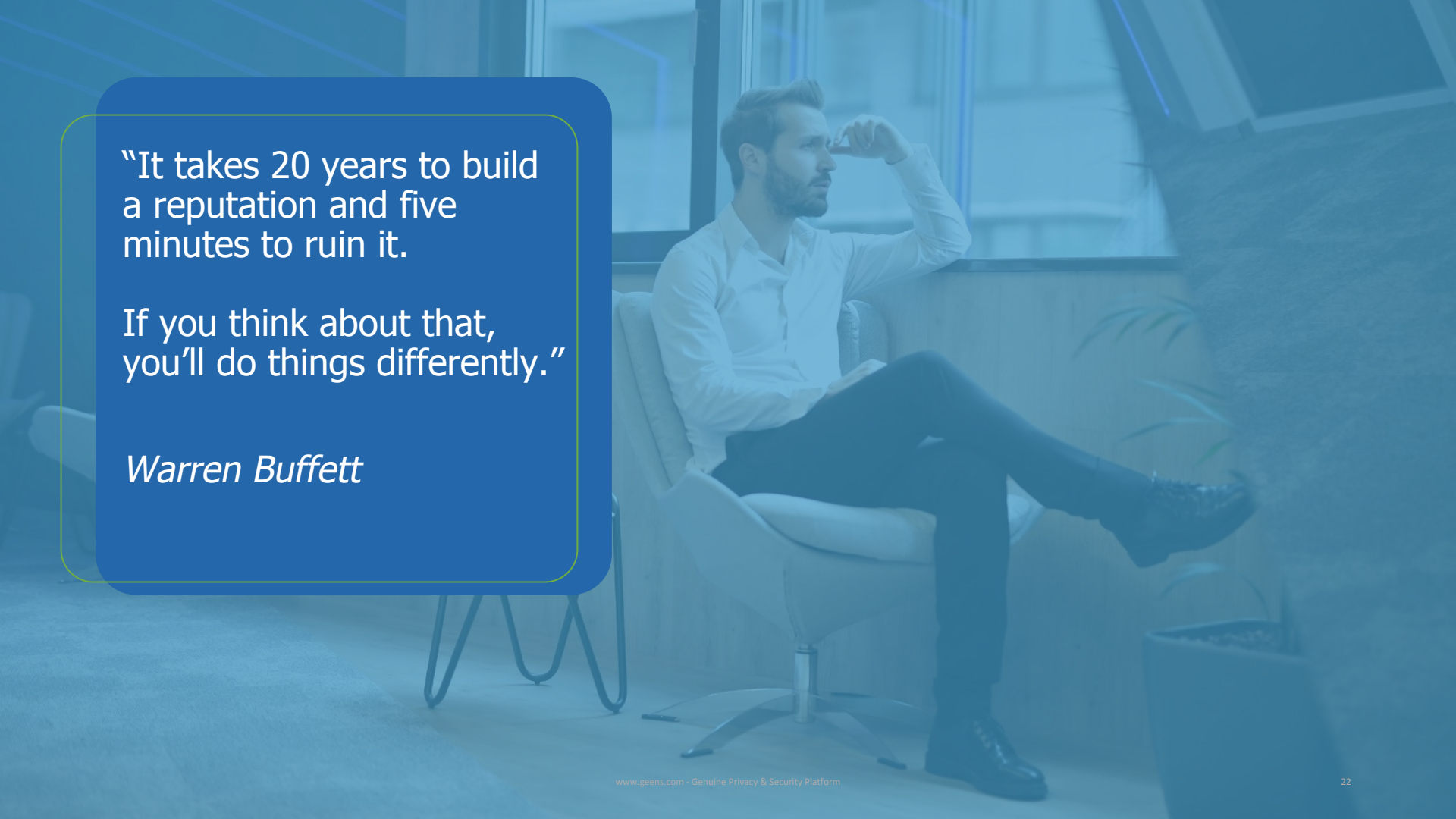
Tax
Don’t have to worry about data security because of the Geens NPO end-to-end encryption and IBM Hyper Protect protocols.

Consulting
Not being dependent on email and FTP sites, employees can easily collaborate internally and send the presentations or large files to the customers.

Risk advisory
Avoiding GDPR incidents, data privacy breaches, authenticity along with optimized and simplified internal audits, information system assurance and data leakage by using RSM data action Log list and smart contracts blockchain timestamping.

Outsourcing
Create a shared folder for each employee containing work orders and instead of sorting through stacks of paper or emails, employees have a clean list in RSM Dashboard of tasks they need to do that day.

Transaction
Collaborate among multiple parties, monitor and take actions based on timestamped deliverables as proof of agreements while ensuring secure and private communication.


"It takes 20 years to build a reputation and five minutes to ruin it.
If you think about that, you'll do things differently."
Warren Buffett

Encrypted Cloud Storage &
Blockchain Timestamping
Gee-nodes on Geens.com

www.geens.com