WHITEPAPER DI XOPERO

STANDARD DI SICUREZZA

Grazie alla criptazione tramite algoritmo 256 bit, due localizzazioni indipendenti dei server ed una combinazione unica dei migliori parametri di sicurezza fisica, possiamo garantire il più alto livello di sicurezza dei dati.

Algoritmo AES 256
Certificato SSL
Ridondanza server
Briefcase
Verifica dei dati

Backup dei dati

- l'applicazione cripta i dati con algoritmo AES 256: i dati sono già criptati all'interno del device dell'utente e trasmessi attraverso il protocollo di sicurezza SSL. E' garantita così una doppia protezione contro il furto dei dati e i ransomware;
- i dati sono immagazzinati in due differenti datacenter ridondati che garantiscono, anche in caso di failure di uno di essi, l'accesso ai dati utente;
- l'applicazione "BRIEFCASE" cripta i dati all'interno del device utente attraverso una chiave separata (diversa da quella utilizzata durante il backup) generata in maniera randomica per una maggiore sicurezza;
- prima di essere immagazzinati nei Datacenter, i file sono divisi in parti più piccole, compressi e criptati prima dell'invio;
- la verifica dell'integrità dei dati avviene in questo modo: durante il processo di invio l'applicazione calcola il checksum per i dati criptati, poi, durante la fase di ripristino, ricalcola il checksum di verifica ed effettua il confronto per tutti i dati.

Chiave di default
Chiave scelta dall'utente

Criptazione

Per garantire il più alto livello di sicurezza dei dati, gli utenti possono scegliere una chiave di criptazione (default o scelta dall'utente) che sarà utilizzata per crittare i dati trasmessi.

La chiave di default è generata automaticamente durante la prima esecuzione dell'applicazione, quindi salvata all'interno dei database utenti nel datacenter: l'utente non può perderla in nessun modo.

L'utente può anche scegliere **una chiave privata personale** per crittare i suoi dati. Questa garantisce un terzo ed elevatissimo grado di protezione ai dati utente, poichè non è salvata in nessun database. Tuttavia in caso di perdita di tale chiave di crittazione il ripristino dei dati criptati dal server non sarà possibile,nemmeno tramite l'intervento diretto di Xopero.

Data center situati in
USA o in Europa

Data Center sicuri

I dati dei nostri clienti sono immagazzinati nei nostri datacenter situati in USA, Germania o Polonia. I dati degli utenti Italiani risiedono nella sede dei datacenter di Asseco in Polonia. Tutti i datacenter sono costruiti appositamente per garantire la massima sicurezza e installati all'interno di aree specifiche. Gli impianti sono progettati nel rispetto di tutte le normative "mission-critical" per la salvaguardia del dato.

- biometria e accesso tramite card;
- 2 localizzazioni indipendenti dei server;
- ridondanza UPS;
- vicinanza agli aeroporti internazionali;
- massima protezione sul rischio di esposizione
- a disastri naturali.