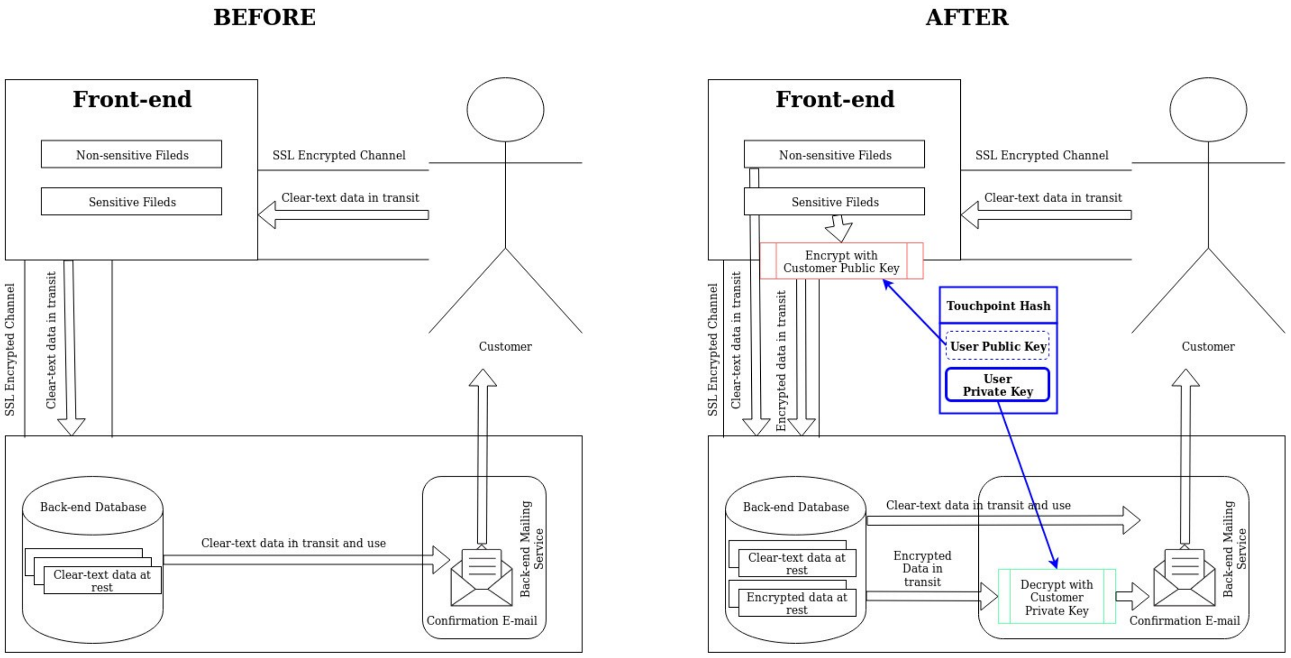
PBD ELLIPTICO

Data Protection framework implementing privacy-by-design principles

PbD Elliptico is an end-to-end data encryption and access management framework that is aimed at covering the current GDPR[2] requirements and at mitigating privacy and security risks. By applying a robust encryption philosophy and transparent key-management facilities, it elegantly solves the most common scenarios faced by companies, while dealing with sensitive user data.



In the above example, we are demonstrating a highly simplified operations model, where the Customer is placing an Order via the Company Front-end and needs to receive an order confirmation via email.

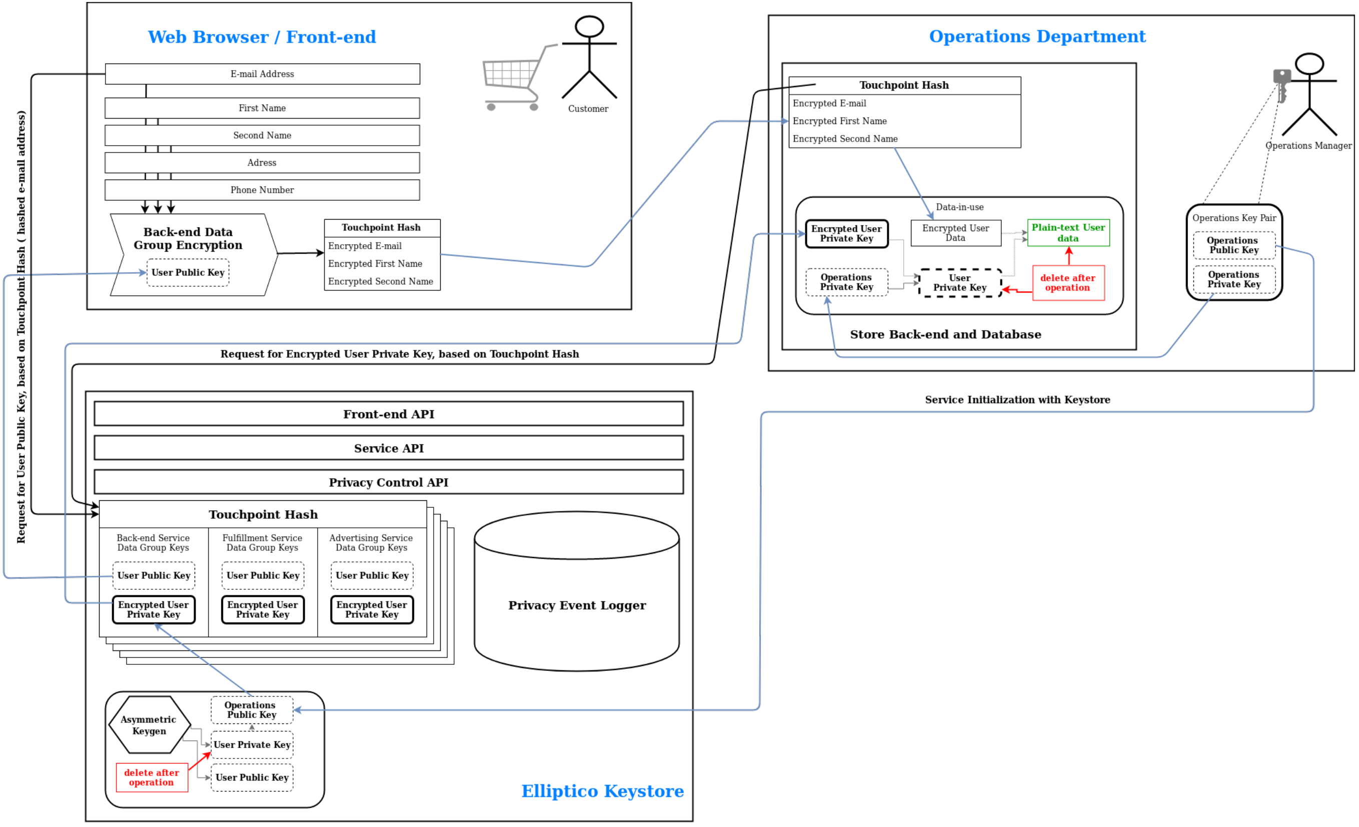
A very high-level explanation shows how Elliptico gets plugged into the process:

- Customer is identified by a Touchpoint Hash generated by the Front-end to get a Customer Public key from Elliptico and to encrypt all the sensitive fields,
- The Back-end receives and stores encrypted data,
- The mailing service, based on the Touchpoint Hash requests the Customer Private Key [*] and decrypts the required sensitive fields.
- Each Customer has a unique key-pair assigned to his Touchpoint Hash

This approach gives multiple advantages:

- Data in Transit and at Rest is encrypted [3]
- Only Data in Use is decrypted and only for the predefined uses
- Customer Private Keys are protected and can’t be stored permanently
- Data Warehousing solutions can still use sensitive data for table linking, but can’t decrypt it
- Customer can request to be forgotten by key-pair deletion

More details on Key distribution and management:



1. The Operations Manager sets-up the Framework by defining the Sensitive Data Groups and the Touchpoint Hash. He also generates a dedicated Operations Public-Private key pair.
2. He sends the Operations Public Key to the Keystore and securely stores the Operations Private Key within the back-end.
3. A customer is ready to finalize an order within the Front-End. He starts filling his e-mail address and other sensitive data. As soon as the e-mail is complete it is hashed and is sent to the keystore with a request for a dedicated Customer Public Key.
4. Within the Front-end, the browser will use the received Customer Public Key to one-by-one encrypt all the sensitive fields and will send them over to the Back-end in the same way it sends non-sensitive data. The Back-end will store the data and wait for the next step.
5. When the Order is complete, the Back-end will have to send a confirmation e-mail, for

which it will have to decrypt the E-mail address and name of the customer. It starts by sending a request for the Encrypted Customer Private key using the Touchpoint Hash as an identifier.

6. The Keystore wills send back the Encrypted Customer Private key, which can then be decrypted within the Back-end using the Operations Service Private Key.
7. The decrypted Customer Private Key is then used to decrypt the customer e-mail and names. After the e-mail is sent, the sensitive data is no longer needed, so the Back-end deletes both the decrypted Customer Private Key as well as the decrypted Customer Data.

For more detailed information, check the complete PbD Elliptico document.