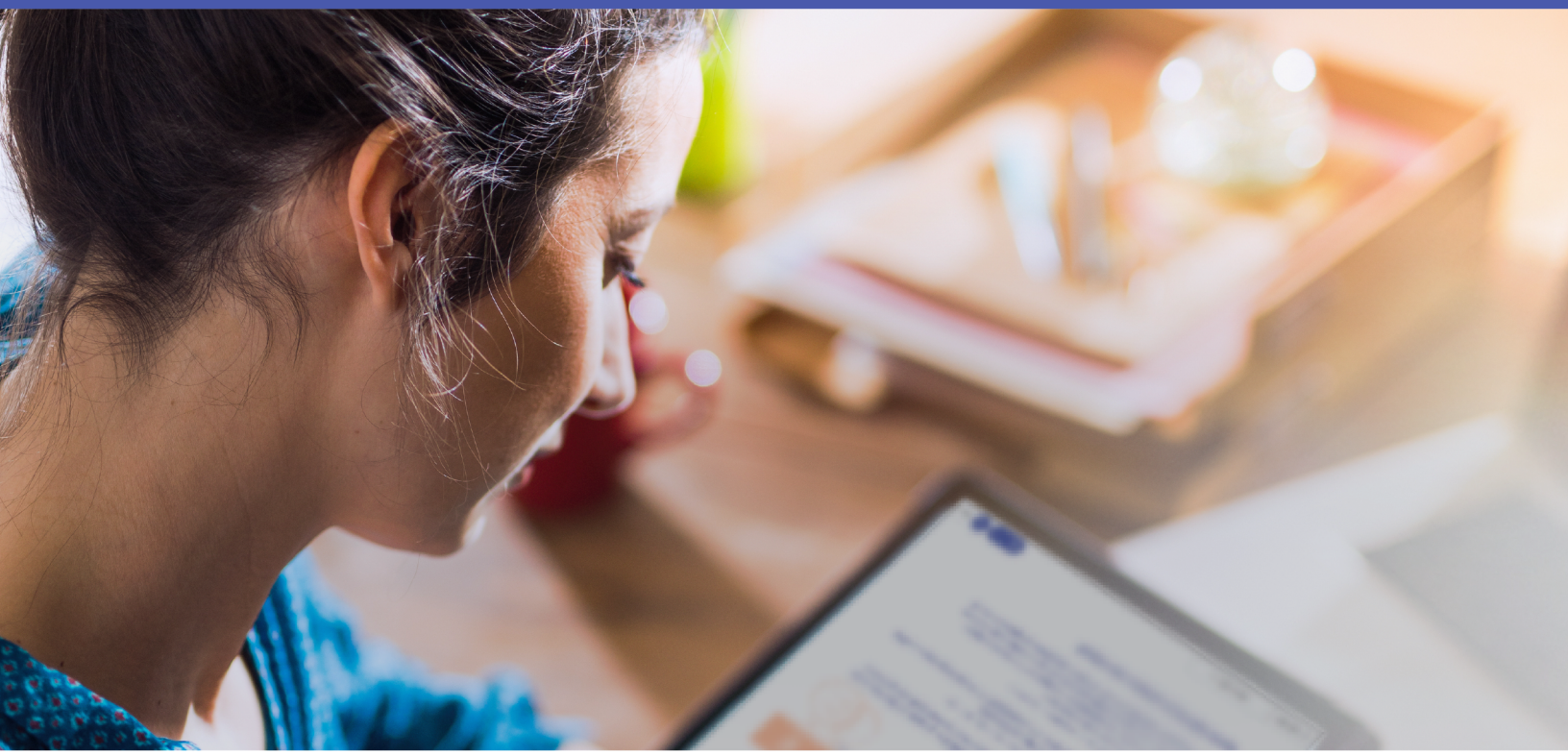
Explain Everything



Security

We take our responsibility to keep your data secure extremely seriously. All communication between your device and Explain Drive is encrypted using SSL (TLS 1.2).

Passwords

Your password is encrypted and never stored in our database in a readable/ unencrypted format. You are responsible for choosing a strong password and keeping it secret.

Employee access

We will only access your account to respond to support requests, and seek your consent before proceeding. The exception is if there is suspected abuse or an urgent security reason.

Credit cards

Explain Everything does not process or store any credit card details belonging to yourself. If you pay for one of our paid plans using your credit card then your payment is processed by a third party, PCI compliant payment processor - Braintree. Your card details are never transmitted through or stored on Explain Everything servers.

Sep 2020

Architecture in more detail

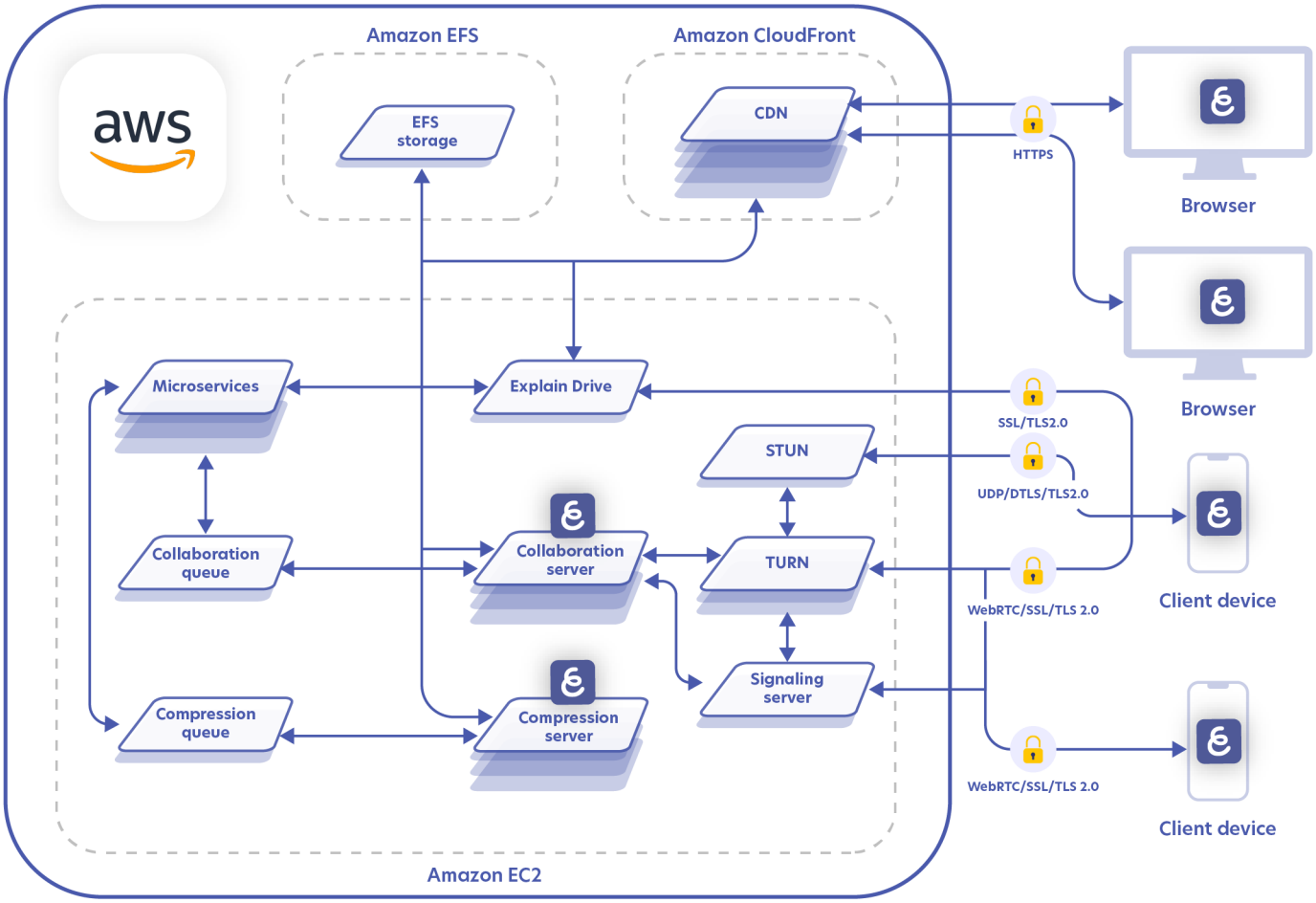
Explain Everything colla boration is based on a universally accepted standard, WebRTC, using encrypted audio and data channels

All communication with the STUN/TURN servers is encrypted. Explain Everything uses its own STUN/TURN and signaling servers that are embedded in the Explain Everything's AWS infrastructure.

Explain Everything project data are stored on Amazon EFS using an encrypted system, where data and metadata are encrypted at rest.

Note

The AWS key management infrastructure uses Federal Information Processing Standards (FIPS) 140-2 approved cryptographic algorithms. The infrastructure is consistent with National Institute of Standards and Technology (NIST) 800-57 recommendations.



The EE infrastructure as of May 1st, 2019

Summary of current EE's infrastructure as pictured on the May 2019 infrastructure diagram

Explain Everything services consist of 3 major parts:

- content storage and management
- collaboration services
- content distribution network

All communication between these elements is encrypted using industry standards. All communication to and from EE's services is also encrypted according to industry standards.

Content storage and management resides within AWS and uses Amazon EFS for storage and Amazon CloudFront as the content distribution network. Project data are stored on Amazon EFS using an encrypted file system, where data and metadata are encrypted at rest.

Servers used for the Explain Drive, MP4 compression service, collaboration and WebRTC connection infrastructure are Amazon's EC2 instances.