Super file(s) transfert !!

Web project / Crypto

You: - "I finish the plateform!!"

New BOOS: - "Super, let's see it !"

Corrections:

If any of these points are not true the correction stops

Name	Description / question
Server	must not be able to access of file and fileNames
Client	encryption and decryption is done only on the client.
Spy	The content of the file must not be accessible even if a spy sees all the exchanges with the server. or if the server is hacked and all these data are stolen.

> *When the site is in production, your very nice **Boss** will give you an SSL certificate. So all your exchanges will be in HTTPS. For convenience, the project does not need to set the https.*

Name	Description / question	number of perc
Navigator	Can we access with the web navigator ?	4
Server don't access	Is it possible for the server to access the files ? (the secret key should not be stored on the server or accessible in logs). the expected answer is no	10
Any size	is it possible to send files of any size ? The browser's memory must not explode.	8
Easy to use	Compatible: firefox 69 / chrome 77 / safari 13.0 ? Only one link is required for downloading. (no password to type). Attention if there is secret key in link, check if the secret key is sended to server	10
Crypto Library	Only native crypto library, and polyfill nodeJs native crypto are authorized. It is forbidden to re-code crypto algorythm.	8
Which algo crypt	Why you choose this algo ? check initialisation vector, Salt and password. Are they unique and random !?	10
multiple files	Can you send multiple files ? When you download, you receive a compressed archive of the sent files ? (archive.zip, archive.tar.gz)	8
Expire Date and download	The owner* can set an expiration date and the maximum number of downloads ?	8
Corruption files	The platform must control the file's integrity (client side)	8
Owner view files	The owner* can view his file(s)	8
Delete	Only the owner* of the file(s) can delete them. Check how	8

	authentification of owner* works. Ex: if is it API Rest, send request delete even if you don't be the owner.	
Protection download/metaData	The server checks if the client has the secret key before sending metaData or Files. Warning! Don't send the secret key to the server	10
BONUS	SLIDER	0-25