Project 3

Alex Wyner

10/30/2022

Project 6-6:

4) Graphical user interface, text, application

Description automatically generated

5) The hash changes completely, not resembling the first hash at all.

7) Block and nonce.

8) Yes, the previous hash for block 5 is identical to the hash of block 4 because that is how block chains ensure integrity of data held in the blockchain. Since each block in the chain holds a hash of the previous block as well as its own hash, if block 5 compares its previous hash to the hash of block 4 and sees they don’t match, it will indicate that the data changed at some point in the chain before or at block 4.

10) Graphical user interface, application

Description automatically generated

This block is now invalid because the data has changed, changing the hash so that it no longer begins with four zeroes.

11) Blocks 4 and 5 are now red because the data in block 4 has changed, and with the current nonce the hash no longer begins with 4 zeroes. Block 5 is invalid because the hash for its previous block is not valid.

13) Graphical user interface, application

Description automatically generated13) Blocks 3, 4, and 5 are all invalid because entering data in block 3 caused its hash to change, resulting in an invalid previous hash in block 4 and 5. This illustrates how the blockchain resists change because if you change a block in the chain, all blocks after it will be invalidated.

14) Graphical user interface, application

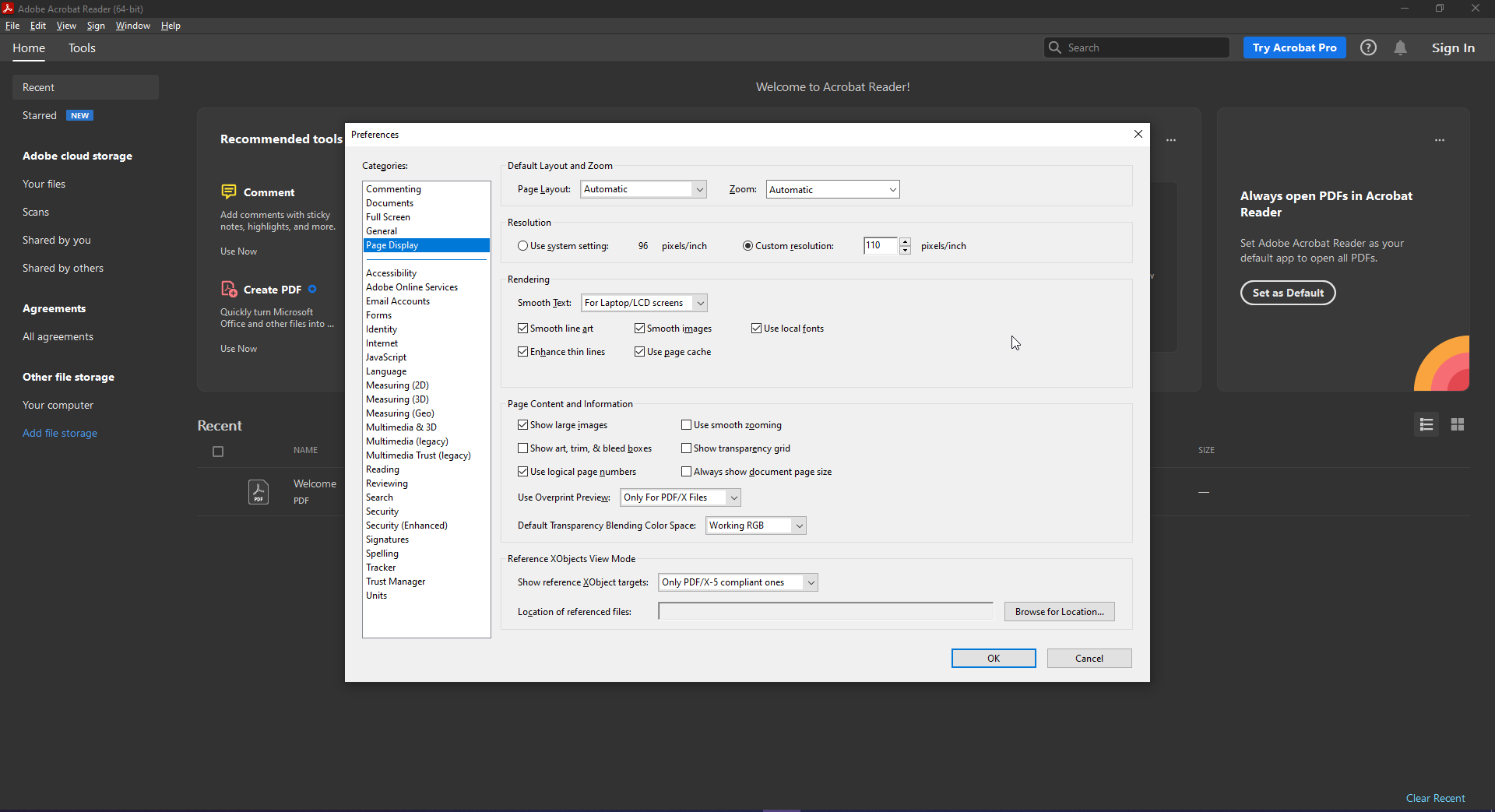
Description automatically generatedAfter clicking mine, block 3 is now valid but 4 and 5 remain invalid.

17) When making a change to block 5, the last block, you only need to mine block 5. If you make a change to block 3, you must mine blocks 3, 4, and 5. Since adding data and then mining a block changes the hash of that block, any blocks that come afterwards will have invalid previous hashes and must be mined as well.

Case Project 6-4: How secure are they? Features? Strengths and weaknesses? Current usage?

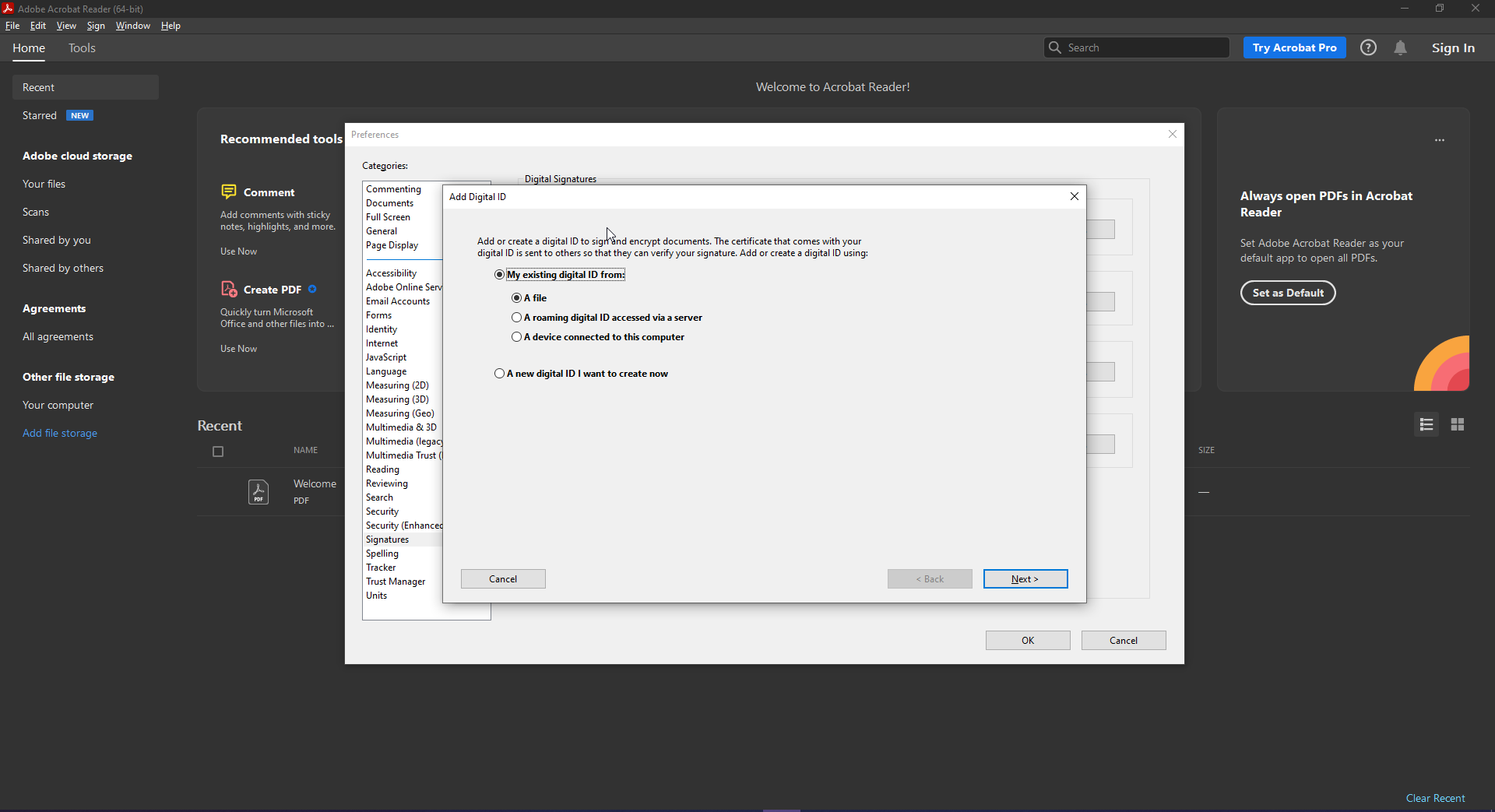
While Twofish and Blowfish are both symmetric encryption algorithms, meaning the decryption algorithm is the same as the encryption algorithm but in reverse and a single key is used to both encrypt and decrypt data, Twofish is generally considered more secure than Blowfish. Twofish was built on Blowfish and was designed to be a more secure version of the existing algorithm. Both algorithms use a block cipher rather than stream cipher, however the Twofish uses a block size of 128 bits rather than Blowfish’s 64 bits, which contributes to Twofish being more secure. Both algorithms undergo 16 rounds of manipulation and encryption, however Twofish has been found to have faster encryption speeds and comparable decryption speeds to Blowfish. The main drawback to Blowfish is that it has been found to be vulnerable to weak keys, whereas Twofish hasn’t had the same problem. Usages for this style of encryption algorithm include encrypting passwords for applications, encrypting hard drives (Truecrypt uses Twofish, bcrypt uses blowfish), and other operations that require high speed encryption and decryption.

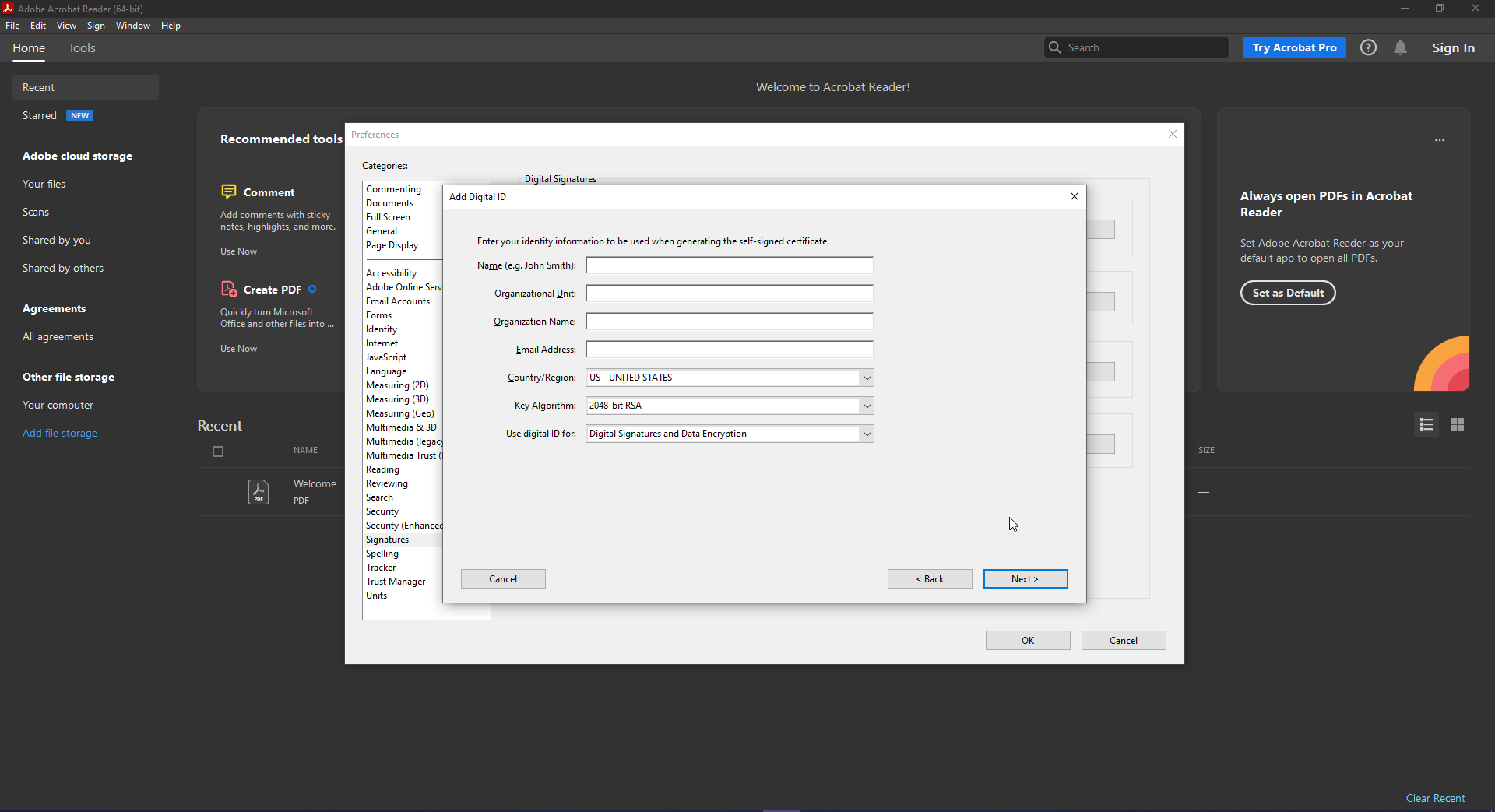
Project 7-4:

7) 

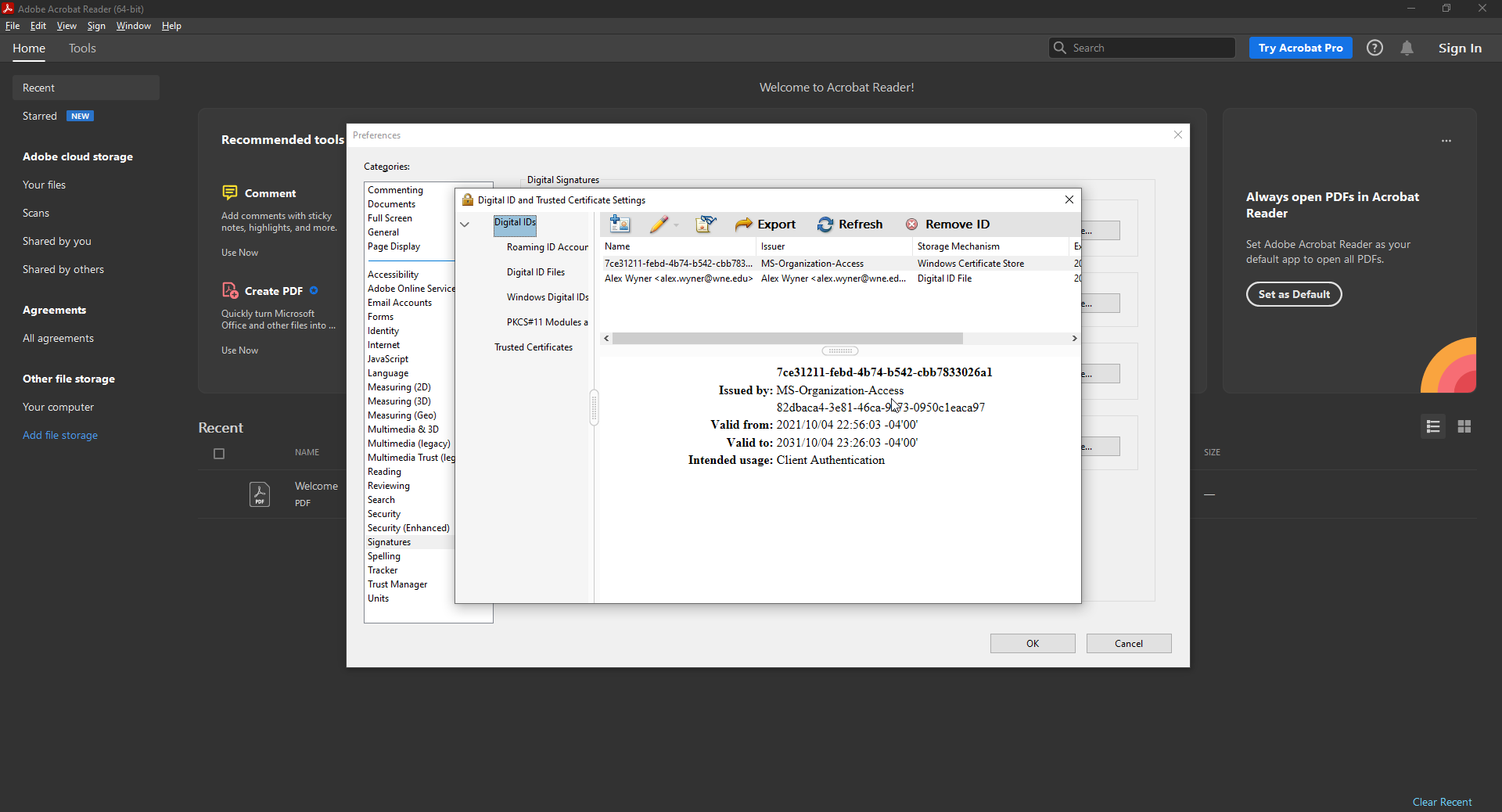
8) A picture containing text, screenshot, monitor, indoor

Description automatically generated

11) 

12) 

13) The file extension for PKCS#12 is .p12 or .pfx.

16) 

Reflection: It was surprisingly easy to create the certificate and prepare it for use with Adobe files, however I don’t see many people using them day to day. I would also like to know if it’s possible to forge these certificates, as there is not much point to an authentication certificate that is easily forged. It would require more research to determine but the main questions I have after this exercise are around the security and ability to prove authenticity of these certificates.

Case Project 7-1:

TLS was developed as a part of the special project Secure Data Network Systems, a joint project involving the NSA, National Bureau of Standards, the Defense Communications Agency, and twelve corporations involved in computers and networks beginning in August of 1986. The first version, originally known as SP4 and later renamed TLS, was published in 1995. SSL was originally meant to provide transport layer security for transmitting data, however version 1.0 had such serious flaws it was never released, SSL 2.0 was released but quickly found to have serious security flaws and was also not compatible with many existing websites, and SSL 3.0 was found to have serious security vulnerabilities in 2014. TLS 1.0 was released as an upgrade to SSL 3.0, fixing many of its security flaws, and subsequent versions TLS 1.1, 1.2, and 1.3 continued to improve security and functionality. Each version of TLS released addressed new attack methods and newly discovered vulnerabilities. As of now I could not find anything about a new TLS version being developed, it appears as though many are still upgrading to either TLS 1.2 or 1.3.