CRYPTOMAThIC
www.cryptomathic.com

Topic Paper - Email Signing

SIGNING AND ENCRYPTING EMAIL SECURELY AND CONVENIENTLY USING CRYPTOMATHIC SIGNER

Signing and encrypting emails improve communication security since it helps ensure non-repudiation. In short, the signed email (when verified) proves to the recipient that you signed the contents of the message and not an imposter, and that the contents have not been altered in transit. The signature includes your certificate and public key. Secure storage of the signing (private) key has always been the issue since only then do we have confidence that an individual really did sign a particular email.

Historically there has been two solutions to this privacy problem: storing the key in a password-protected file or generating and storing the private key within a smart card or USB token. Because password-protected key files offer limited resistance, most companies chose to give their employees smart cards or USB tokens containing a private key used for email signing and decryption. The private key is stored within the chip on the local device and the owner authorises use of the key by inserting the device into a reader and supplying a passphrase to the requesting application (typically a mail client).

In recent years, smart card solutions have become increasingly expensive to maintain. Modern laptops and PCs do not have a smart card reader built into them, so external card readers must be purchased and attached. Mobile devices certainly don't have card readers, meaning that encrypted emails cannot be read whilst on the move. The era of using smart cards for digital signatures is over. In addition, the new USB standard (type C) and virtualisation technologies that are largely deployed in corporate environments make the existing USB devices unusable. Now is a very good time for re-considering your email signing technology.

CENTRALISED SIGNING

Consider the problem of securely storing money: most households do not invest in expensive strong-boxes or safes to securely store cash. Instead, they delegate that task to a central authority (a bank), who invests in world-class security infrastructure to protect the assets of thousands of people. To access his money, a customer simply has to prove his identity to the bank.

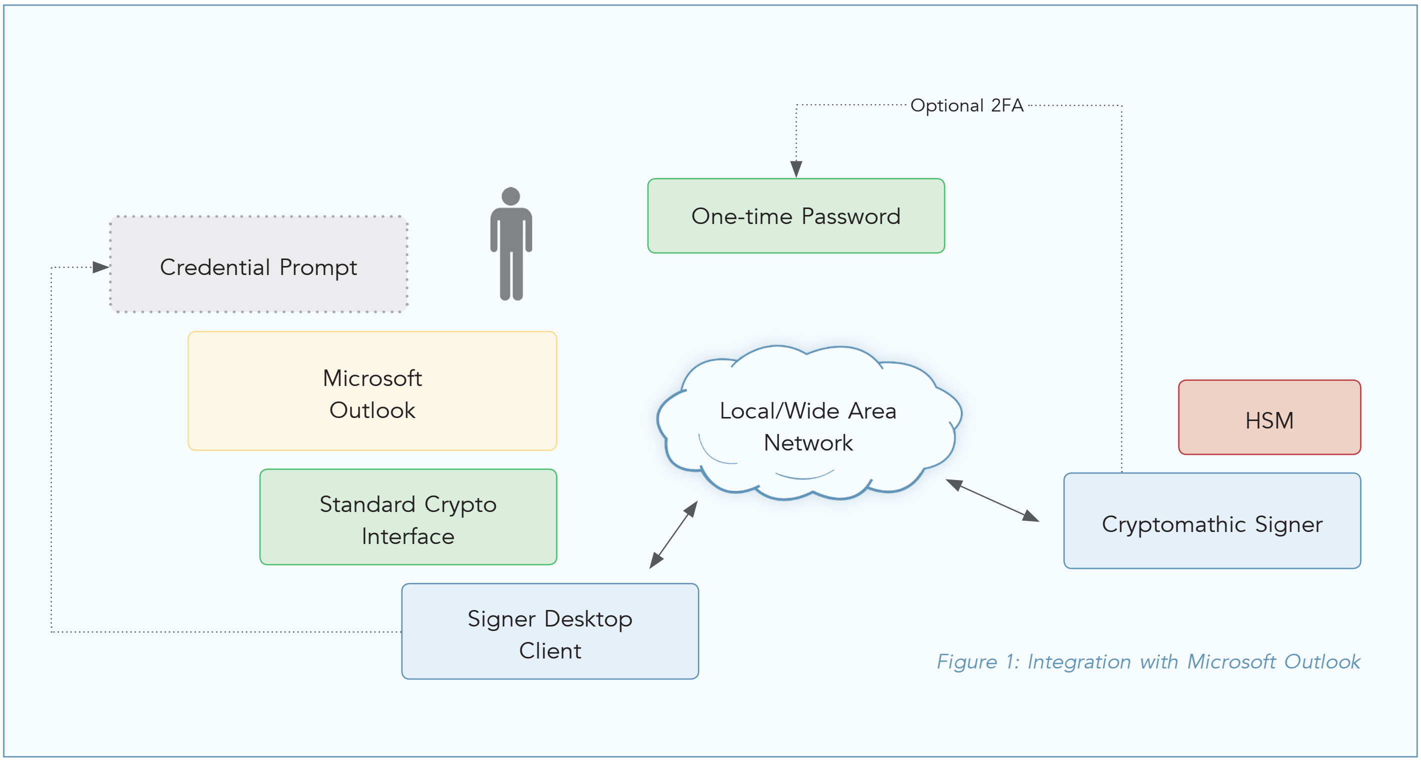


Figure 1: Integration with Microsoft Outlook

This is exactly how Cryptomathic Signer works. Instead of requiring users to store their private keys locally on their device, Signer uses a central hardware security module (HSM) to securely store the keys of every employee in the company. In order to use his private key from an application, a user simply connects to the central Signer server and authenticates himself. The crypto operation is then performed using the central HSM and the result is returned securely to the user. Because asymmetric crypto operates on very small amounts of data, there is very little network traffic bouncing back and forth from the Signer server.

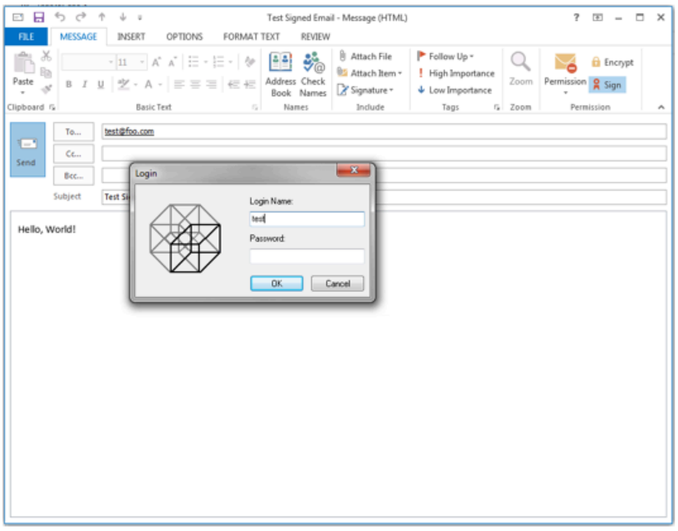
Users can authenticate themselves to Signer using a wide range of popular one- and two-factor mechanisms, including static and dynamic/OTP passwords using common standards such as OATH. Companies can adopt a suitable authentication strategy based on their security and risk policies.

As an added benefit, centralised signing provides very strong revocation guarantees. Unlike the traditional smart card approach, which relies on certificate revocation lists, a centralised signing service can immediately “switch off” usage of a key for a particular user when his credentials are compromised or when he is no longer trusted.

INTEGRATION WITH OUTLOOK

Cryptomathic Signer can integrate with most common business applications, including Microsoft Office and Adobe PDF Reader. The integration is made possible thanks to a small application called the Signer Desktop Client. This application registers itself as a crypto provider, so it can be used by programs such as Microsoft Outlook for signing and decrypting emails. The Signer Desktop Client sends data to the Signer server for processing and provides the visual prompts for user credentials. The integration between the various system components is shown in Figure 1 (Page 1).

On a technical level, Signer Desktop Client presents an MSCAPI interface, which Outlook can use to perform crypto operations. When the user logs into Signer for the first time, the Windows certificate store is populated with the certificates associated with the user’s private keys. Whenever Outlook tries to use the private key corresponding to the certificate, Signer Desktop Client is invoked and handles the operation.



Test Signed Email - Message (HTML)

To... test@foo.com

Subject Test Si

Hello, World!

Login

Login Name: test

Password:

Figure 2: Prompting for credentials

Figure 2 shows Signer Desktop Client prompting the user for authentication credentials. If the private key requires a second factor of authentication, the user is then prompted to enter a second piece of information (e.g. a one-time password). To avoid the user repeatedly entering his credentials, the Signer Desktop Client will keep the user logged in for a period of time (in one application) before automatically logging him out.

CONCLUSION

Cryptomathic Signer offers a compelling replacement for legacy smart cards or USB tokens. The cost of deployment is lowered because there is no requirement for specialized hardware for end-users. For this same reason, mobile users can also benefit from the same centralised signing solution; something that is impossible in a smart card solution.

ABOUT CRYPTOMATHIC

Cryptomathic is a world leading provider of IT security solutions to businesses across a wide range of industry sectors, including banking, cloud, government, mobile and technology. Solutions are predominantly based on secure server infrastructure embracing secure hardware (HSMs), with the purpose of solving specific and dedicated problems in the likes of EMV, digital signatures, lifecycle key management, managed cryptography, mobile devices and PKI.

Founded in 1986, Cryptomathic prides itself on strong technical expertise and unique market knowledge, with 2/3 of employees working in R&D, including an international team of security experts and a number of renowned cryptographers. At the leading edge of security provision within key markets, Cryptomathic closely supports its global customer base with many multinationals as longstanding clients.

Learn more at cryptomathic.com