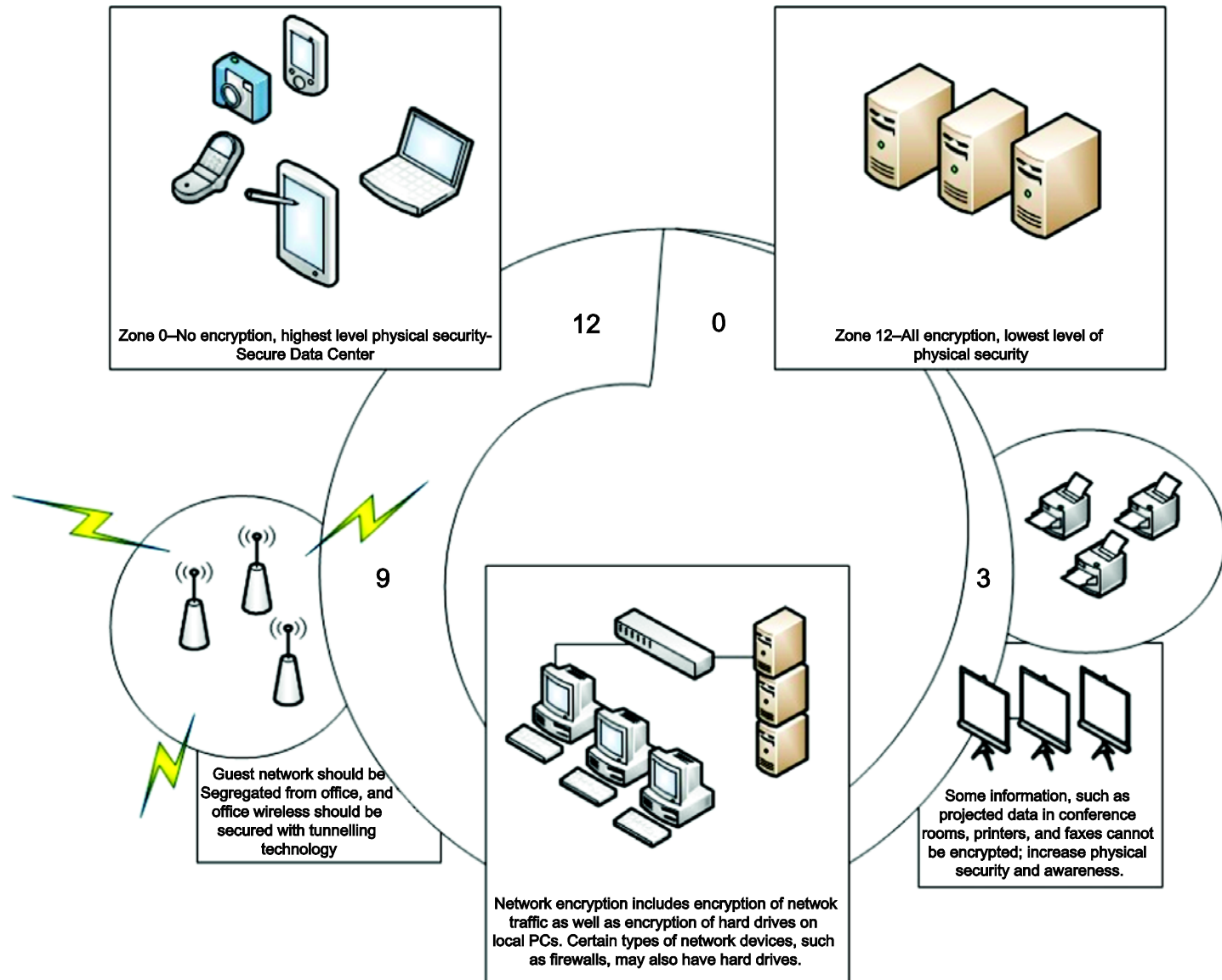
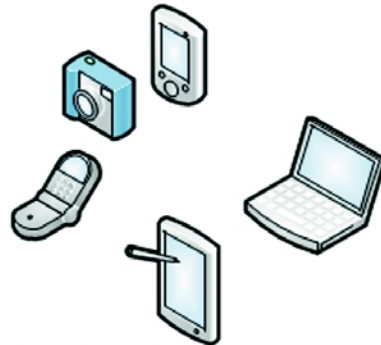


Chapter 63

Fundamentals of Cryptography



f63-01-9780123943972



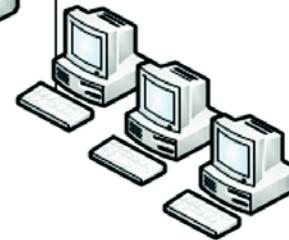
Zone 12 - Mobility: PKC and SKC Due to lowest level of physical security, remote wiping capabilities, self data destruction or increased physical security. Whole drive encryption.



Zone 3 - Server/Datacenter: SKC technology. With a higher level of physical security, virtual access points that are vulnerable are encrypted. Shares and other high visibility items are encrypted. Any segments with Internet exposure are encrypted, as is sensitive data.



Zone 9 - Wireless Security: PKC: Network encryption includes encryption of network traffic as well as encryption of hard drives on local PCs. Certain types of network devices, such as firewalls, may also have hard drives.

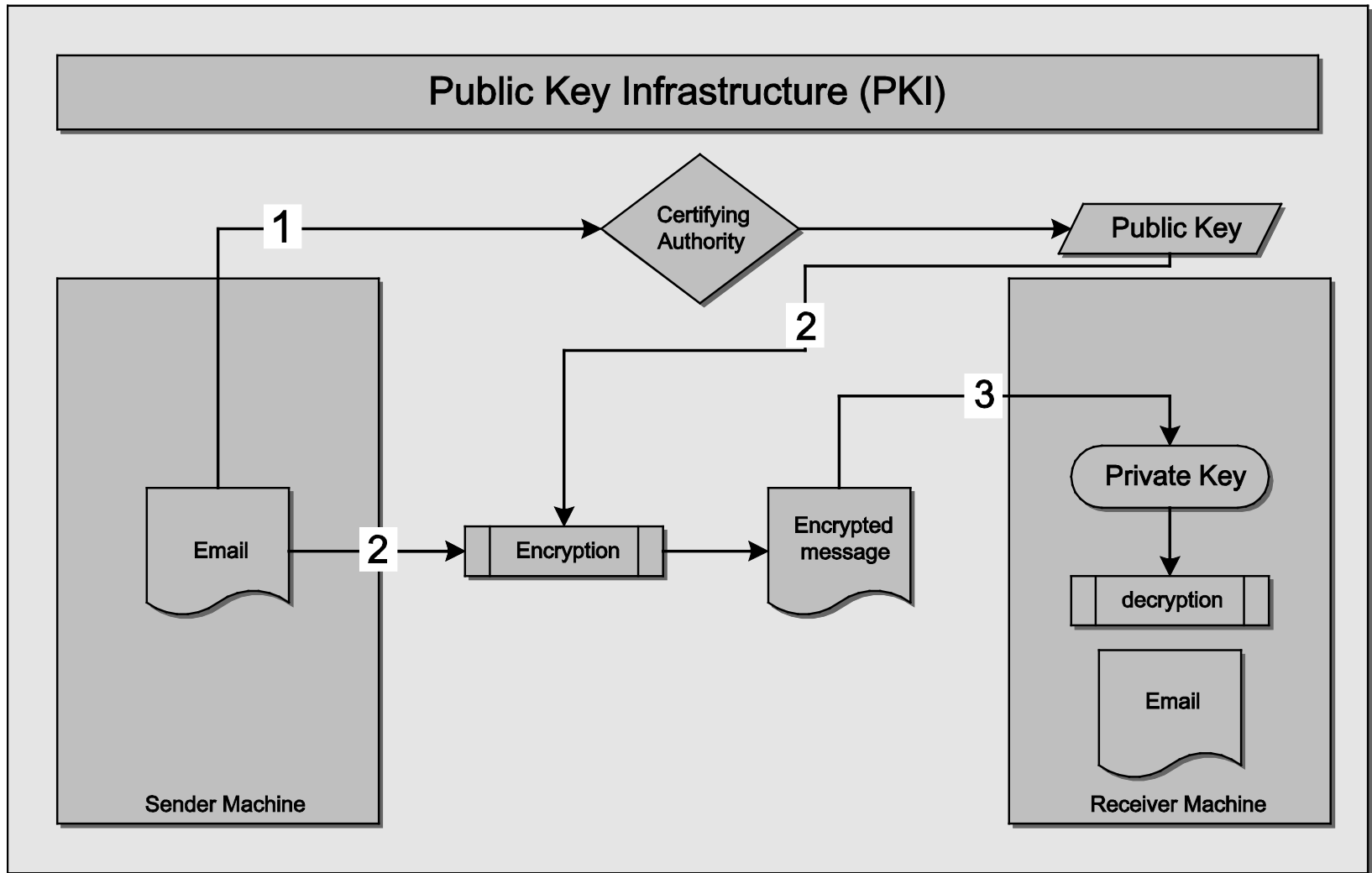


Zone 6 - Desktop: Blend of SKC and PKC technologies. Network encryption includes encryption of network traffic as well as encryption of hard drives on local PCs. Certain types of network devices, such as firewalls, may also have hard drives.

Zone 7 - Desktop Email: leverages PKC for all sensitive email communications. A policy is developed to group all external communications into this zone, with a comprehensive policy that covers encryption and creates a standard.

In this reference, the dock-face approach is used to assign zones to each element of the infrastructure. It is segmented by the mobility and physical security of the device, and the operating network, as well as by the possibility of exposure of the data to external elements, such as external email recipients.

f63-02-9780123943972



f63-03-9780123943972