# IPR2022-00114 (Patent 11,063,766)
# IPR2022-00113 (Patent 10,992,480)
# PGR2022-00007 (Patent 10,992,480)

Patent Owner Demonstratives

# Concerning claims 1, 3-5, 8-13, and 21-33 of U.S. Patent No. 11,063,766 (the '766 Patent)

**Ellison**

(57) **ABSTRACT**

The present invention is a method and apparatus to protect a subset of a software environment. A key generator generates an operating system nub key (OSNK). The OSNK is unique to an operating system (OS) nub. The OS nub is part of an operating system in a secure platform. A usage protector uses the OSNK to protect usage of a subset of the software environment.

**'766 Patent**

(57) **ABSTRACT**

A method for performing an electronic transaction is disclosed. The method provides authentication data and authentication software to an electronic device and preferably stored in a secure storage location or other location inaccessible to the user or the operating system of the device. When digital data is requested from a transaction party that requests a digital signature, the authentication software is activated to generate said digital signature from the authentication data. Next, the digital signature is provided to the other transaction party, which then provides the requested digital data. The digital signature may be embedded in the requested and provided digital data. Further, a method for performing a verification of legitimate use of digital data is disclosed. Digital data digitally signed according to the present invention may only be accessed if the embedded digital signature is identical to a regenerated digital signature that is regenerated by the authentication software, using user inaccessible authentication data installed on the device. If the embedded and regenerated digital signatures are not identical, the data may not be accessed and an error signal is generated.

DEMONSTRATIVE EXHIBIT-NOT EVIDENCE 2

# Concerning claim 1 of the '766 Patent

**'766 Patent:**

1. A method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the electronic device having an operating system creating a run-time environment for user applications and authentication software running in a separate operating environment, independent from and inaccessible to the operating system, the electronic device having a memory comprising storage locations, part of the memory being accessible to the operating system, part of the memory being a secure area,

wherein the electronic device comprises a system for accessing a memory location in the memory, wherein the system for accessing the memory location is configured to selectively report the storage locations of the secure area, wherein the storage locations are not reported to the operating system while at the same time being reported to the authentication software running in the separate operating environment, the method comprising:

providing a private key in the secure area of the electronic device which private key is inaccessible to a user of the electronic device, wherein the secure area is inaccessible to the operating system of the electronic device, thereby rendering the private key inaccessible to the user;

providing authentication software in the electronic device, the private key being accessible to the authentication software, wherein the authentication software is stored in the secure area inaccessible to the operating system;

activating the authentication software to generate a digital signature from the private key, wherein the authentication software is run in a secure processing environment inaccessible to the operating system; and

providing by the electronic device the digital signature to the second transaction party.

DEMONSTRATIVE EXHIBIT-NOT EVIDENCE 3

## Concerning claim 1 of the '766 Patent

**'766 Patent – Figure 3**

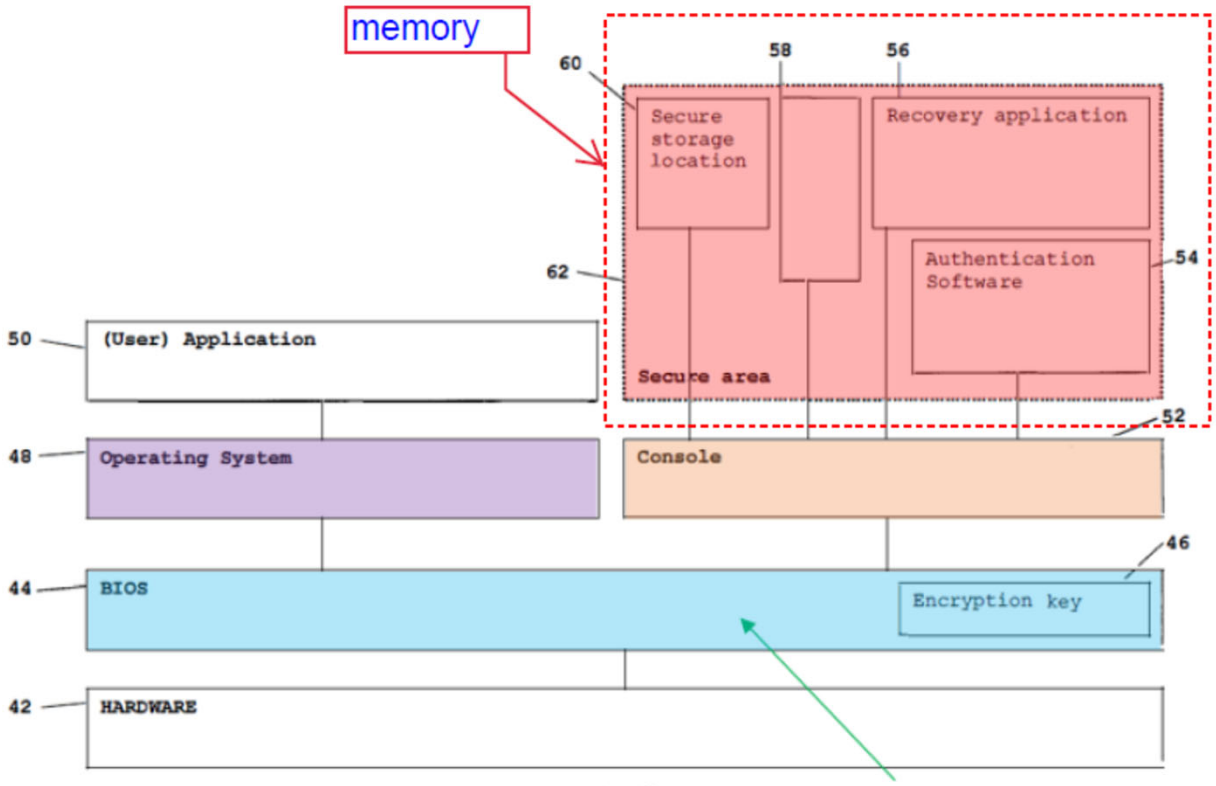



FIG. 3

BIOS 44 may block OS 48 from accessing console 52 and secure area 62

DEMONSTRATIVE EXHIBIT-NOT EVIDENCE 4

## Concerning claim 1 of the ‘766 Patent

**Ellison – Figure 1A**

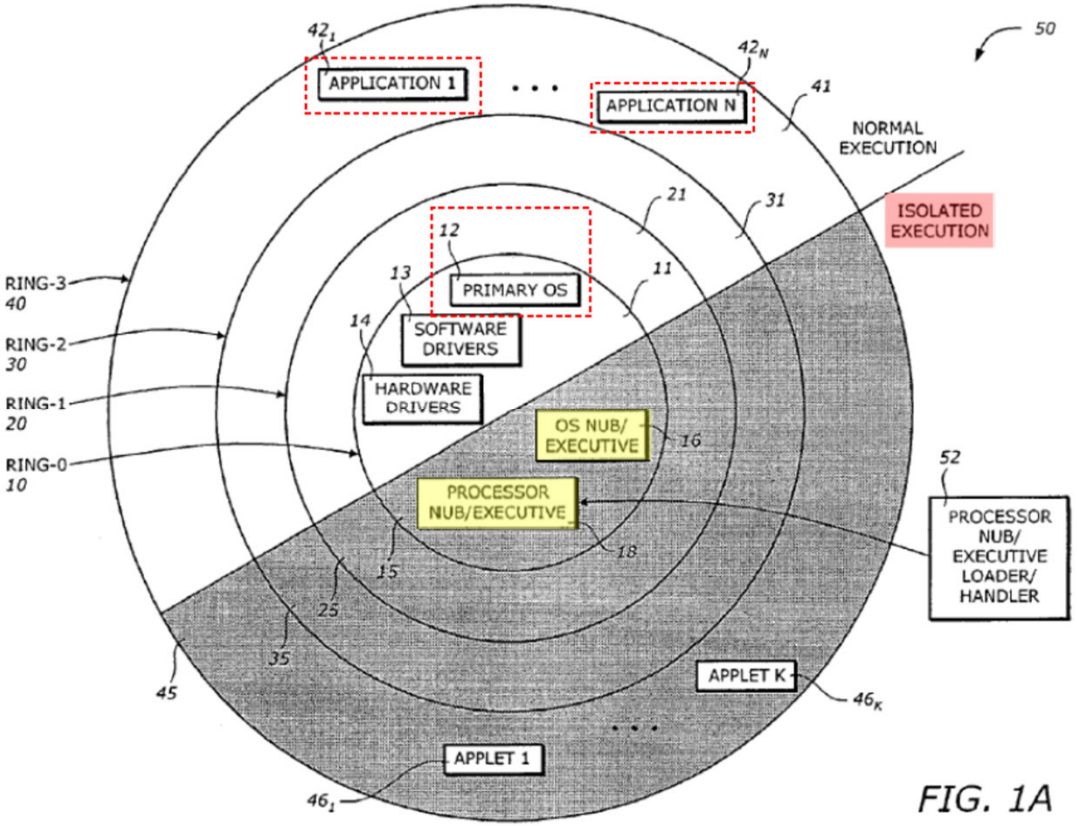



FIG. 1A

DEMONSTRATIVE EXHIBIT-NOT EVIDENCE 5

## Concerning claim 1 of the ‘766 Patent

**Ellison – Figure 1B**

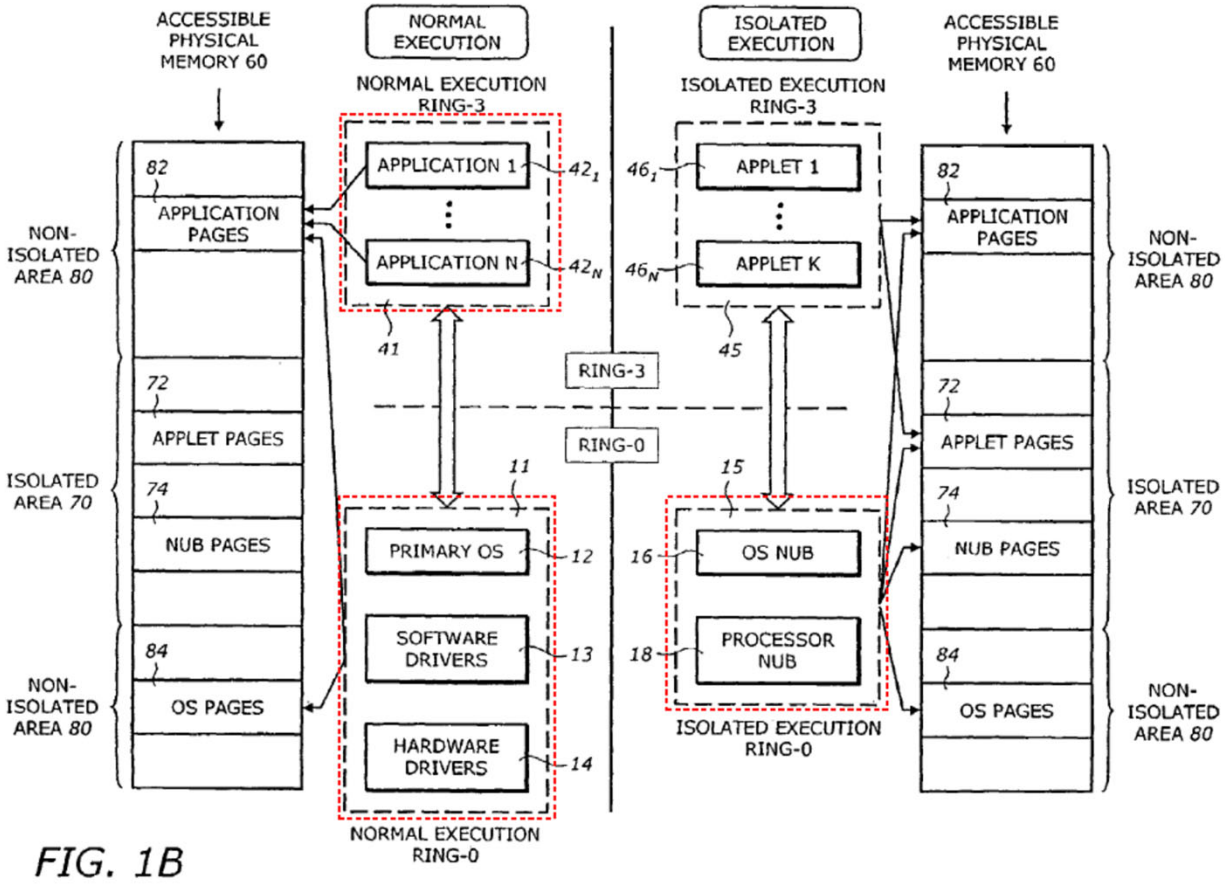



FIG. 1B

DEMONSTRATIVE EXHIBIT-NOT EVIDENCE 6

# Concerning claim 1 of the ‘766 Patent

## Ellison – Figure 1C

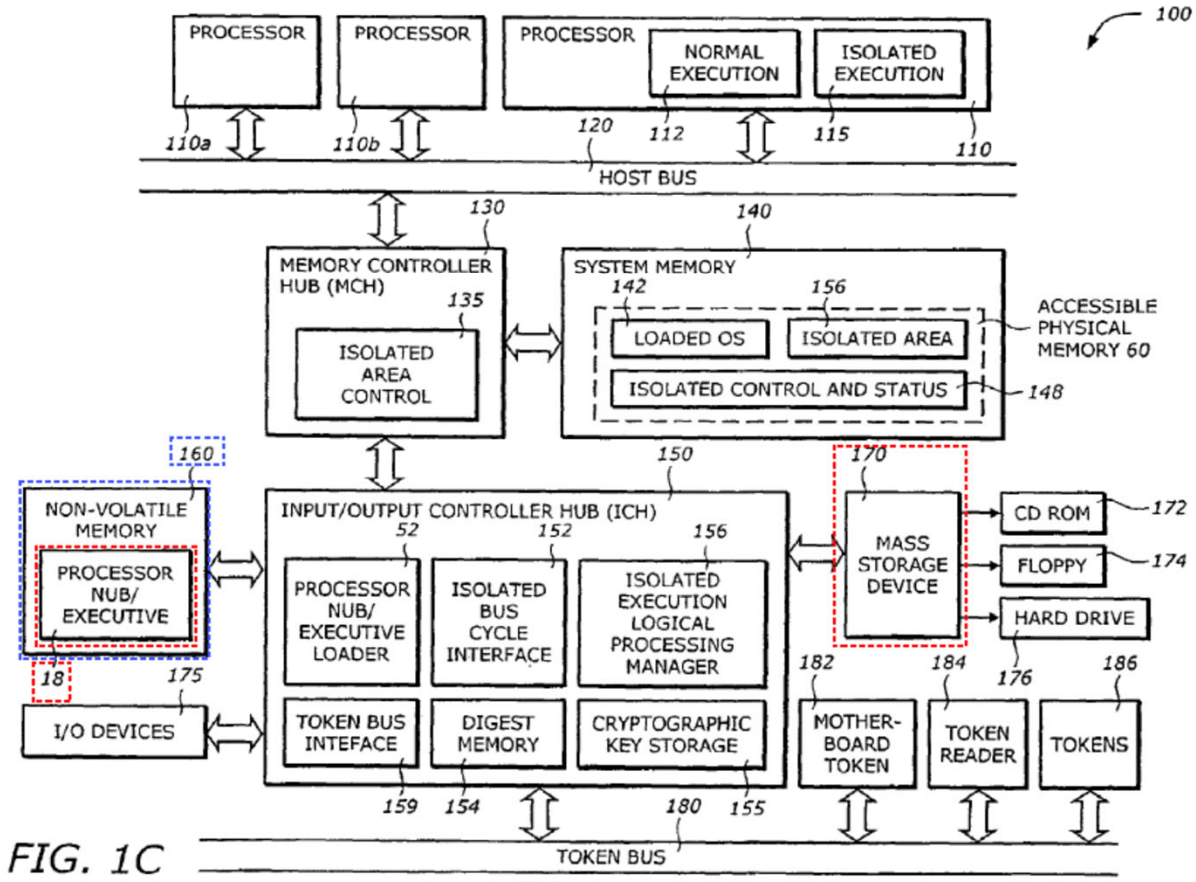



FIG. 1C

## Ellison – Col. 7, lines 32-58

The mass storage device **170** stores archive information such as code (e.g., processor nub **18**), programs, files, data, applications (e.g., applications $\mathbf{42}_1$ to $\mathbf{42}_N$), applets (e.g., applets $\mathbf{46}_1$ to $\mathbf{46}_K$) and operating systems. The mass storage device **170** may include compact disk (CD) ROM **172**, floppy diskettes **174**, and hard drive **176**, and any other magnetic or optical storage devices. The mass storage device **170** provides a mechanism to read machine-readable media. When implemented in software, the elements of the present invention are the code segments to perform the necessary tasks. The program or code segments can be stored in a processor readable medium or transmitted by a computer data signal embodied in a carrier wave, or a signal modulated by a carrier, over a transmission medium. The “processor readable medium” may include any medium that can store or transfer information. Examples of the processor readable medium include an electronic circuit, a semiconductor memory device, a ROM, a flash memory, an erasable programmable ROM (EPROM), a floppy diskette, a compact disk CD-ROM, an optical disk, a hard disk, a fiber optical medium, a radio frequency (RF) link, etc. The computer data signal may include any signal that can propagate over a transmission medium such as electronic network channels, optical fibers, air, electromagnetic, RF links, etc. The code segments may be downloaded via computer networks such as the Internet, an Intranet, etc.

## Concerning claim 1 of the ‘766 Patent

**Ellison – Figure 2**

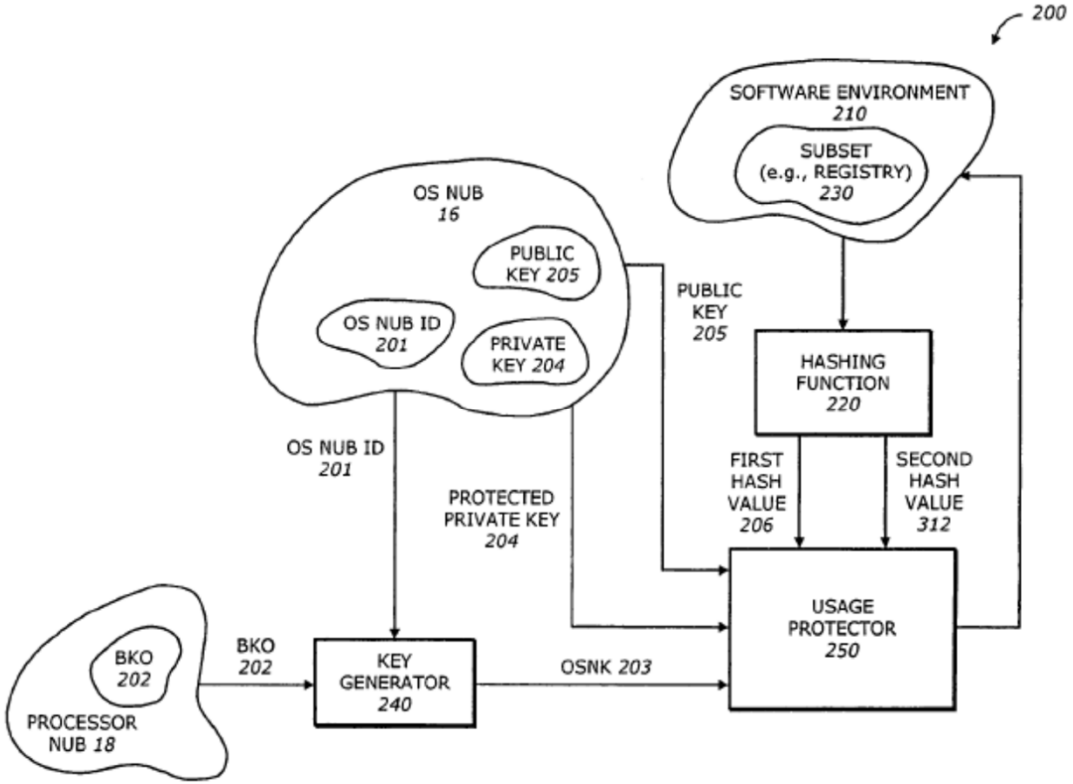



FIG. 2



EXHIBIT 2013
IPR2022-00113, IPR2022-00114, PGR2022-00007
Samsung v Ward Participations B.V.

## Concerning claim 1 of the ‘766 Patent

**Ellison – Figure 3C**

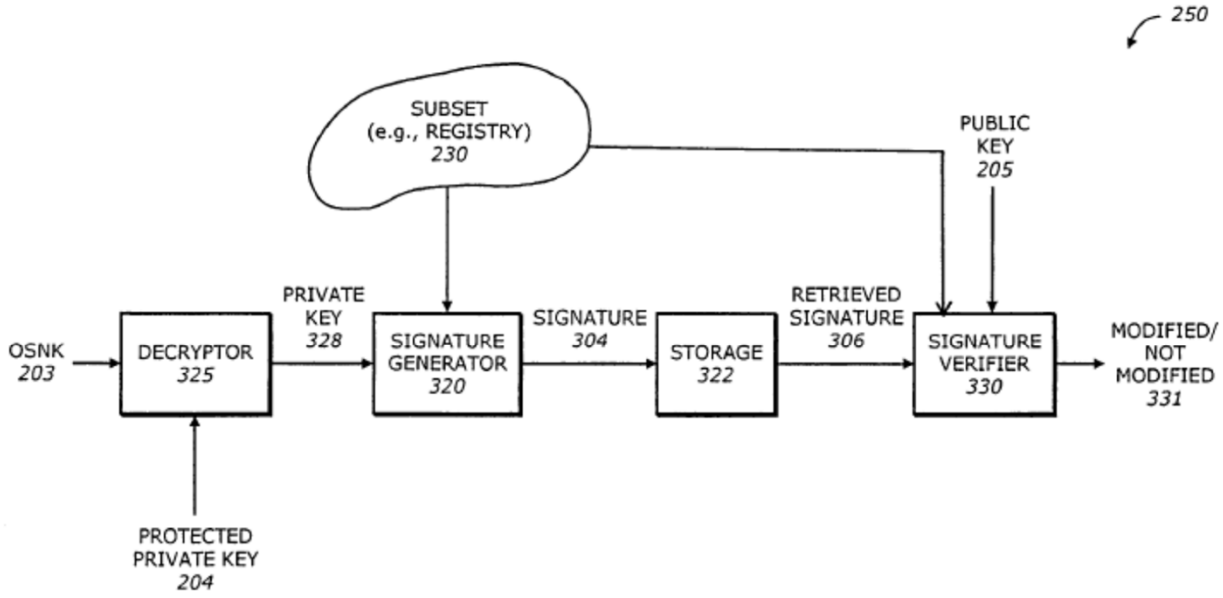


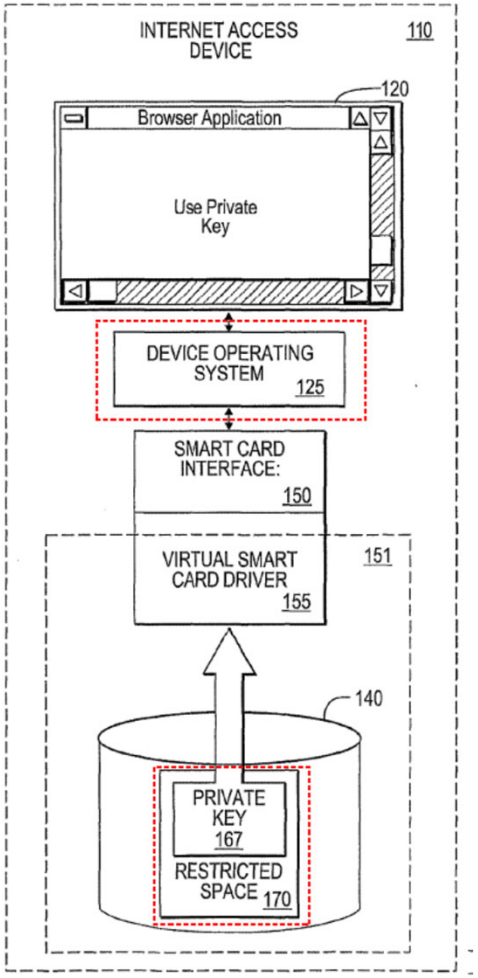

FIG. 3C



EXHIBIT 2013
IPR2022-00113, IPR2022-00114, PGR2022-00007
Samsung v Ward Participations B.V.

# Concerning claim 1 of the ‘766 Patent

Muir – Figure 3




Muir – Page 9

Virtual smart card driver 155 uses such restricted memory 170 to store private keys 167. Virtual smart card driver 155 may further use restricted memory space 170 to store encrypted and decrypted data. In one embodiment, the restricted memory space 170 is on the hard drive. In another embodiment, restricted memory space 170 may be any type storage media, i.e. random access memory (RAM), read-only memory (ROM), electrically erasable programmable ROM (EEPROM), flash memory, compact disc (CD), CDROM, floppy, etc.

Private key 167 is data that is unique to a specific user. Private key 167 may be used in a public-key (PK) infrastructure. Alternatively, private key 167 may be used in a secret key infrastructure. Private key 167 may be used for a

-9-

# Concerning claims 1, 3, 6, 11, and 14-19 of U.S. Patent No. 10,992,480 (the '480 Patent)

1. A method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the electronic device having an operating system creating a run-time environment for user applications, the method comprising:

providing a private key in a memory of said electronic device, said memory being a secure part of a Basic In Out System or any other secure location in said electronic device, which private key is inaccessible to a user of said electronic device, wherein the private key is encrypted when the private key is stored in said memory, a decryption key for decrypting the private key being incorporated in the electronic device, said decryption key being inaccessible to said user, to any user-operated software and to said operating system, wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the private key inaccessible to said user, wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software;

providing authentication software in said electronic device, the private key being accessible to said authentication software, wherein authentication software is stored in said secure memory inaccessible to said operating system;

activating the authentication software to generate a digital signature from the private key, wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

providing the digital signature to the second transaction party.

DEMONSTRATIVE EXHIBIT-NOT EVIDENCE 11

## Concerning claim 1 of the ‘480 Patent

**Ellison – Figure 1C**

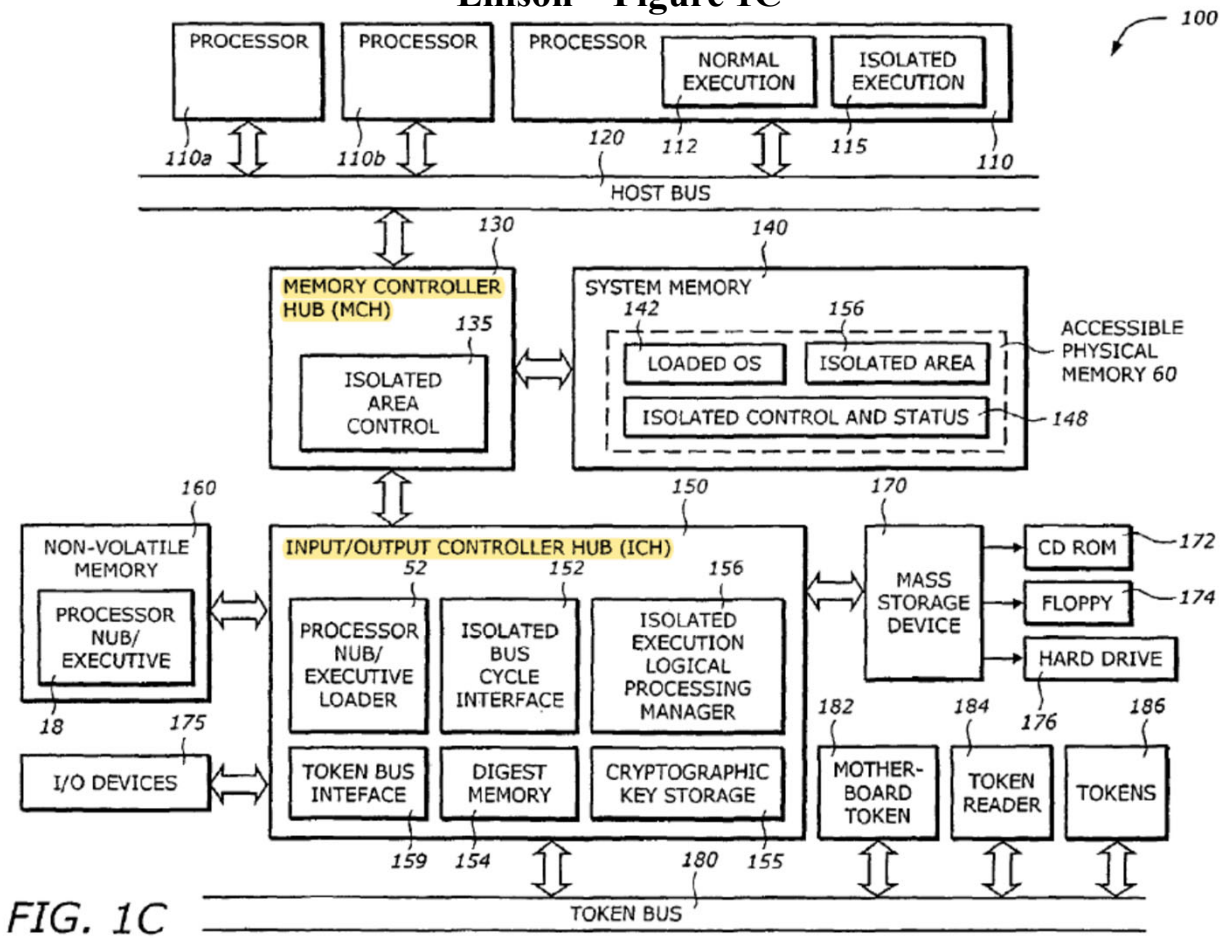



FIG. 1C



EXHIBIT 2013
IPR2022-00113, IPR2022-00114, PGR2022-00007
Samsung v Ward Participations B.V.

## Concerning claim 1 of the ‘480 Patent

**Ellison – Figure 1A**

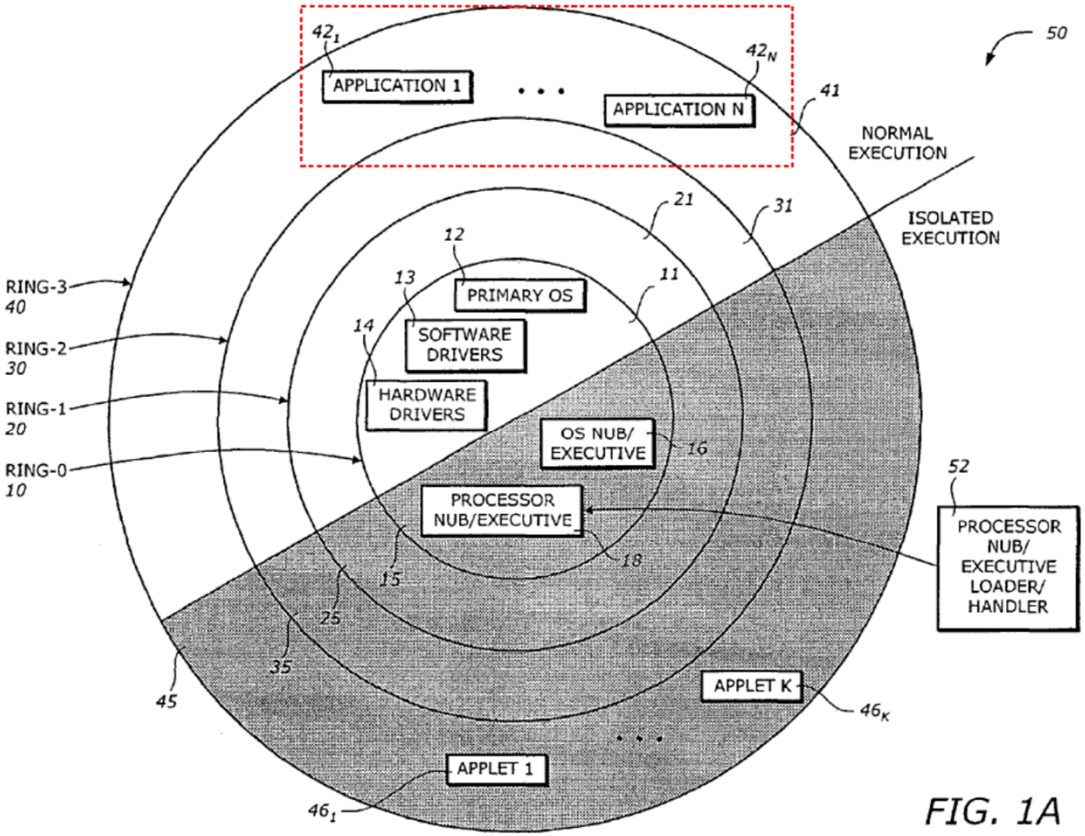



FIG. 1A



EXHIBIT 2013
IPR2022-00113, IPR2022-00114, PGR2022-00007
Samsung v Ward Participations B.V.

## Concerning written description for the claims of the ‘480 Patent

**Decision to Grant PGR – Excerpt, page 11**

PGR2022-00007
Patent 10,992,480 B2

not reasonably convey to an artisan of ordinary skill that the inventor had possession of 1) “providing a private key in a memory of said electronic device, wherein said memory being a secure part of a Basic In Out System or any other secure location in said electronic device operated by the first transaction party,” wherein 2) “[the] private key is inaccessible to a user of said electronic device,” wherein 3) “the private key is encrypted when the private key is stored in said memory,” and wherein 4) “the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software,” as required by claim 1. *See* Ex. 1001, 17:64–18:29.



EXHIBIT 2013
IPR2022-00113, IPR2022-00114, PGR2022-00007
Samsung v Ward Participations B.V.