# judgment

**DISTRICT COURT THE HAGUE**

Commercial matters

**Judgment of 13 May 2020**

in Case C/09/576280 v HA ZA 19-713 (Case I) of

**DTS INTERNATIONAL B.V.,**
at Laren,
plaintiff in the main action,
defendant in the counterclaim action,
attorney at law, Mr. W.E. Pors, The Hague,

against

**1. SAMSUNG ELECTRONICS BENELUX B.V.,**
in Delft,
**2. SAMSUNG ELECTRONICS EUROPE LOGISTICS B.V.,**
in Rijswijk,
**3. SAMSUNG ELECTRONICS OVERSEAS B.V.,**
at Amsterdam,
defendants in the main action,
claimants in the counterclaim action,
attorney at law B.J. Berghuis van Woortman in Amsterdam,

and in the case with case number / docket number C/09/577703 / HA ZA 19-793 (Case II**)**

of

**DTS INTERNATIONAL B.V.,**
at Laren,
plaintiff in the main action,
defendant in the counterclaim action,
attorney at law, Mr. W.E. Pors, The Hague,

against

**1. SAMSUNG ELECTRONICS BENELUX B.V.,**
**in** Delft,
**2. SAMSUNG ELECTRONICS EUROPE LOGISTICS B.V.,**
in Rijswijk,
**3. SAMSUNG ELECTRONICS OVERSEAS B.V.,**
in Amsterdam,
defendants in the main action,
claimants in the counterclaim action,
attorney at law B.J. Berghuis van Woortman in Amsterdam.

In both cases, plaintiff in the main action, defendant in counterclaim, will hereinafter be referred to as DTS. Defendants in the main action, counterclaimants, will hereinafter, in both cases, be referred to separately as Samsung Electronics Benelux, Samsung Electronics Europe and Samsung Electronics Overseas and jointly as Samsung c.s.

The case is handled for DTS by the aforementioned lawyer, mr. T.M. van den Heuvel, mr. ir. K. Hsia and S.A. Lodder, attorneys at law in The Hague, and dr. ir. S.M. van Rijnswou, patent attorney, and for Samsung c.s. by the aforementioned attorney at law, mr.ir. M.W. de Koning and D.M. Termeulen, attorneys at law in Amsterdam.

**The proceedings**

1.1. The course of the proceedings in Case I follows from:
- the order of the Interim relief judge of this Court of 23 May 2019 to sue under the accelerated regime for proceedings on the merits in patent litigation;
- the writ of summons of 5 June 2019;
- the submission of DTS exhibits EP01 to EP34;
- statement of answer in the main action, also counterclaim, also request to apply confidentiality regime, with exhibits GP01 to GP27;
- the statement of answer in counterclaim, with exhibits EP35 to EP39;
- the submission of additional exhibits by DTS, with exhibits EP40 up to and including EP69;
- the submission of further exhibits by Samsung c.s., with exhibits GP28 up to GP32;
- the submission of responsive exhibits by DTS, with exhibits EP71 to EP80;
- the submission of responsive exhibits by Samsung c.s., with exhibit GP33;
- the submission of DTS's overview of legal costs;
- the e-mail message from Samsung c.s. of 31 January 2020 with an overview of legal costs (GP34) attached;
- the submission of additional exhibits by DTS, with exhibits EP81 to EP83;
- the submission of further responsive exhibits by Samsung c.s., with exhibit GP35;
- Samsung c.s.'s e-mail message of 10 February 2020 in which they make it known that, to the extent that DTS would like to rely during the oral hearing on its submissions EP82B and EP83C, Samsung c.s. object to this;
- Samsung c.s.'s e-mail message of 12 February 2020 with an up-to-date overview of the costs of the proceedings attached (GP36);
- the submission of additional costs of proceedings of DTS;
- the pleadings of 14 February 2020 and the pleading notes used on that occasion by the parties, whereby marginal numbers 160 and 214 up to and including 250 of the DTS pleadings were not submitted and marginal numbers 4.68 up to and including 4.70 of the Samsung or Samsung's pleadings were not submitted.

1.2. The course of the proceedings in Case II follows from:
- the order of the Interim relief judge of this Court of 23 May 2019

to sue under the accelerated regime on the merits in patent cases;
- the writ of summons of 5 June 2019;
- the submission of exhibits of DTS, with exhibits EP01 to EP34;
- the statement of answer in the main action, also the counterclaim, also the request to apply the confidentiality regime, with exhibits GP01 to GP24;
- the statement of answer in the counterclaim action, with exhibit EP38[1];
- the submission of additional exhibits by DTS, with exhibits EP41 to EP78;
- the submission of further exhibits by Samsung c.s., with exhibits GP25 to GP30;
- the submission of responsive exhibits by Samsung c.s., with exhibit GP31;
- the submission of responsive exhibits by DTS, with exhibits EP79 to EP83;
- the submission of costs, also with exhibit EP84 by DTS (this exhibit concerns the part of the pleading notes as presented by DTS during the oral argument in Case I);
- the submission of additional exhibits by Samsung C.S., with exhibit GP32 (this exhibit concerns Samsung C.S.'s pleadings in Case I, including the unsubmitted parts) and exhibit GP33 (litigation costs);
- the submission of the additional legal costs of DTS;
- the e-mail message from Samsung c.s. of 12 March 2020 with exhibit GP34, an additional overview of legal costs;
- the pleadings of 13 March 2020 and the pleading notes used on that occasion by the parties, which did not include the pleading notes of DTS marginal 33.

1.3. During the oral argument in case II, it was agreed with the parties that the District Court will also take into account all arguments that have been exchanged in case II when assessing case I and vice versa.

1.4. In both cases judgment has been given.

**The facts in both cases**

*Parties*

2.1. DTS concentrates - among other things - on the technical and commercial exploitation of the intellectual property rights transferred to it from Ward Participations B.V. (hereinafter: Ward).

2.2. Samsung Electronics Benelux, Samsung Electronics Europe and Samsung Electronics Overseas all belong to the Samsung group, which is active in the field of computers, software, electronic and telecommunication equipment.

*EP 3 229 099 and EP 1 634 140*

DTS is the proprietor of European patent EP 3 229 099 ('EP 099'), the grant of which was published on 29 August 2018, and of European patent EP 1 634 140

[1] Exhibits 35, 36, 37, 39 and 40 are left blank

(hereinafter referred to as 'EP 140' and, together with EP 099, 'the patents'), the grant of which is published on 16 January 2019. Both patents, as evidenced by the abbreviation (in the authentic English text), relate to a 'method and system for performing a transaction and for performing a verification of legitimate access to, or use of digital data' and apply to the Netherlands, Belgium, Switzerland, Germany, Denmark, Spain, Finland, France, United Kingdom, Ireland, Italy and Sweden. EP 140 was granted on the basis of PCT application PCT/NL2004/000422, published as WO 2004/111752 ('WO 752'). EP 099 was granted on the basis of a divisional application of EP 140. Compared to EP 099, EP 140 is therefore also referred to as the parent patent below. The application for EP 140 and the application for EP 099 were both filed invoking priority of the PCT application PCT/NL03/00436, which was filed on 13 June 2003. EP 099 and EP 140 were transferred from Ward to DTS after they were granted.

2.4. Initially, the examining division of the European Patent Office (EPO) refused the grant of EP 140 for lack of inventive step. In its decision of 11 October 2016, the Examining Division considered an auxiliary request from Ward:

> 7 A request replacing the second auxiliary request during oral proceedings was not admitted into the proceedings. The examining division exerted its discretion under Rule 137(3) to not accept the amendments introduced with this request for the following reasons:
>
> -The amendments are late filed.
>
> -The amendments prima facie do not comply with Article 123(2) EPC.

And further on the same auxiliary request:

> 7.4 Furthermore the description discloses the authentication data and software being unreachable and unknown to the operating system only in connection with the BIOS providing the function of controlling these no other possible entity is disclosed. The features are therefore inextricably linked to the BIOS performing these functions instead and cannot be taken out independently (see Guidelines for Examination in the EPO H-V-3.2.1)

2.5. An appeal against this refusal has been lodged by Ward with the Technical Board of Appeal (TBA) of the EPO. The Technical Board of Appeal subsequently annulled the decision of the Examining Division in its decision of 6 February 2018 (T 0248/17). The TBA's decision contains the following considerations on the conduct of the appeal proceedings:

> IV. In an annex to a summons to oral proceedings, the board informed the appellant of its preliminary opinion that claim 1 of the two pending requests lacked novelty or inventive step. A number of terminological issues were also addressed.

VI. During the oral proceedings, which took place on 6 February 2018, the appellant withdrew all pending requests and filed an amended claim 1 as a new request. It further reserved the right to adapt the claims previously on file and the description.

VII. Claim 1 reads as follows:

"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 a Basic In Out System and an operating system creating a run-time environment for user applications, the electronic device having a memory comprising storage locations, part of the memory being accessible to the memory of the operating system, part of the memory being a secure area of the Basic In Out System, storage locations of which are not reported to the operating system by the Basic In Out System, the method comprising:

providing authentication data in the secure area of said electronic device which authentication data are inaccessible to a user of said electronic device, wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;

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

activating the authentication software to generate a digital signature from the authentication data, 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."

and about the inventive step of claim 1 (according to the auxiliary request):

6.8 The board thus concludes that the subject-matter of claim 1 shows an inventive step over D12 alone (Article 56 EPC 1973), by virtue of the feature that the BIOS "shields" the secure area from the operating system.

The TBA then referred the case back to the Examining division for further consideration of the application, after which Ward changed the claims to the current claims. Subsequently, EP 140 was granted.

2.6. Samsung c.s. opposed to both the granting of EP 099 and the granting of EP 140 at the EPO.

*EP 099*

2.7 EP 099 contains an independent method claim (Claim 1) and 21 claims dependent on that claim, an independent system claim (Claim 23), an independent product claim (Claim 24) and one claim dependent on that product claim.

2.8. The claims of EP 099 in the authentic English version are as follows:

1. 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 authentication data 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 authentication data are inaccessible to a user of said electronic device, wherein the authentication data are encrypted when the authentication data are stored in said memory, a decryption key for decrypting the authentication data 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 authentication data inaccessible to said user;
providing authentication software in said electronic device, the authentication data 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 authentication data, 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.

2. Method according to claim 1, wherein the authentication data are provided by the second transaction party, which stores the authentication data together with data identifying the first transaction party.

3. Method according to claim 2, wherein the second transaction party uses the stored authentication data to obtain transaction specific authentication data according to a specific algorithm.

4. Method according to claim 3, wherein the second transaction party verifies the digital signature provided by the first transaction party using the authentication data stored at the second transaction party.

5. Method according to claim 1, wherein the authentication software has its own unique serial number, software ID and/or private encryption key.

6. Method according to any of the preceding claims, wherein the authentication data are encrypted by the second transaction party using an encryption key before the authentication data are provided to the first transaction party.

7. Method according to claim 6, wherein the authentication software retrieves a decryption key associated with the encryption key and decrypts the authentication data at its first use.

8. Method according to claim 1, wherein the authentication software is installed in an application environment in the secure area such that it may obtain the authentication data without passing through an unsecured part of said electronic device.

9. Method according to any of the preceding claims, wherein the authentication data are encrypted using at least two encryption layers.

10. Method according to any of the preceding claims, wherein the authentication data are encrypted using an encryption key which is associated with a hardware device serial number.

11. Method according to any of the preceding claims, wherein the authentication data are encrypted using an encryption key which is associated with a user identifying number, in particular a personal identifying number, PIN, are a number or a template associated with a fingerprint of the user.

12. Method according to any of the preceding claims, wherein the decryption key is associated with one or more serial numbers of hardware components of said electronic device.

13. Method according to any of the preceding claims, wherein the authentication data is decrypted by the authentication software.

14. Method according to any of the preceding claims, wherein the authentication data is decrypted by an application stored in the electronic device using a device specific encryption key.

15. Method according to any of the preceding claims, wherein the authentication data is decrypted using a decryption key associated with any identifying characteristic, in particular a serial number, a personal identification number, PIN, are a fingerprint of a user.

16. Method according to any of claims 11 to 15, wherein the authentication data are decrypted in a secure processing environment inaccessible to said user and to any user-operated software.

17. Method according to any of the preceding claims, wherein the authentication data comprise an authentication table.

18. Method according to claim 17, wherein the authentication table is generated from a bit string which is generated from fixed data and variable data.

19. Method according to claim 18, wherein the variable data comprise a random table.

20. Method according to claim 19, wherein the random table is calculated from a random two dimensional or three-dimensional pattern.

21. Method according to claim 1, further comprising identifying the user of the electronic device before activating the authentication software.

22. Method according to any one of the preceding claims, wherein the authentication software has a private encryption key for encrypting digital data.

23. System for performing an electronic transaction between a first transaction party and a second transaction 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 system comprising:
means for providing authentication data 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 authentication data are inaccessible to a user of the electronic device, wherein the authentication data are encrypted when the authentication data are stored in said memory, a decryption key for decrypting the authentication data 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 authentication data inaccessible to said user;
means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software, wherein the authentication software is stored in a secure memory location inaccessible to said operating system;
means for activating the authentication software to generate a digital signature from the authentication data, wherein the authentication software is run in a secure processing environment inaccessible to said operating system; and
means for providing the digital signature to the second transaction party; and
means for providing digital data from the second to the first transaction party.

24. Electronic device for performing an electronic transaction between a first transaction party, and a secend transaction party, wherein the electronic device is operated by the first transaction party, the electronic device having an operating system creating a run-time environment for user applications, the electronic device comprising: a memory storing authentication data, said memory being a secure part of a Basic In Out System ar any other secure location in said electronic device, which authentication data are

inaccessible to a user of the electronic device, wherein the authentication data are encrypted when the authentication data are stored in said memory, a decryption key for decrypting the authentication data 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 authentication data inaccessible to said user; a memory storing authentication software, the authentication data being accessible to said authentication software, wherein the authentication software is stored in a secure memory location inaccessible to said operating system;
means for activating the authentication software to generate a digital signature from the authentication data, wherein the authentication software is run in a secure processing environment inaccessible to said operating system; and
means for providing the digital signature to the second transaction party.

25. Electronic device according to claim 24, wherein the electronic device is a personal computer, a cellular phone, a hand-held personal digital assistant with wireless communication capabilities, or a device containing a BIOS.

2.9 In the (undisputed) Dutch translation, the claims of EP 099 are as follows:

1. Procedure for conducting an electronic transaction between a first transactional party and a second transactional party using an electronic device operated by the first transactional party, where the electronic device has an operating system that creates a run-time environment for user applications:
provision of authentication information in a memory of the said electronic device, where the said memory is a secure part of a Basic In Out System or any other secure location in the said electronic device, which authentication information is inaccessible to a user of the said electronic device, where the authentication information is encrypted when the authentication information is stored in the said memory, where a decryption key for decryption of the authentication information is embedded in the electronic device, where the said decryption key is inaccessible to the said user, to any user-operated software and to the said operating system, where the said memory is inaccessible to the said operating system of the said electronic device, making the authentication data inaccessible to the said user, providing authentication software in the said electronic device, where the authentication data is accessible to the said authentication software, where authentication software is stored in the said secure memory inaccessible to the said operating system, activating the authentication software to generate a digital signature from the authentication data, where the authentication software is run in a secure processing environment inaccessible to the said operating system,
provide the digital signature to the second party to the transaction.

2. Working method according to claim 1, where the authentication data are provided by the second transaction party, who stores the authentication data together with data provided by the third party.

identify the first transaction party.

3. Working method according to claim 2, where the second transaction party uses the stored authentication data to obtain transaction-specific authentication data according to a specific algorithm.

4. Working method according to claim 3, in which the second transaction party verifies the digital signature provided by the first transaction party using the authentication data stored with the second transaction party.

5. Working method according to claim 1, whereby the authentication software has its own unique serial number, software ID and/or secret encryption key.

6. Operation according to one of the previous claims, whereby the authentication data are encrypted by the second transaction party using an encryption key before the authentication data are provided to the first transaction party.

7. Working method according to claim 6, in which the authentication software retrieves a decryption key associated with the encryption key and decrypts the authentication data when they are first used.

8. Procedure according to Claim 1, whereby the authentication software is installed in an application environment in the secure area in such a way that it can obtain the authentication information without going through an unsecured part of the said electronic device.

9. Procedure according to one of the previous claims, whereby the authentication data is encrypted with at least two layers of encryption.

10. Procedure according to one of the previous claims, where the authentication data is encrypted with an encryption key associated with a hardware device serial number.

11. Operation according to one of the previous claims, whereby the authentication data are encrypted with an encryption key associated with a user identification number, in the bee without a personal identification number, PIN, or a number or template associated with a fingerprint of the user.

12. Procedure according to one of the above claims, where the decryption key is associated with one or more serial numbers of hardware components of the said electronic device.

13. Working method according to one of the previous claims, in which the authentication data are decrypted by the authentication software.

14. Procedure according to one of the above claims, whereby the authentication data are decrypted by an application stored in the said electronic device with a device-specific encryption key.

15. Procedure according to one of the previous claims, in which the authentication data are decrypted with a decryption key associated with an identifier, in particular a serial number, a personal identification number, PIN, or a fingerprint of a user.

16. Operation in accordance with one of claims 11 to 15, whereby the authentication data are decrypted in a secure processing environment that is inaccessible to the said user and to any user-operated software.

17. Procedure according to one of the previous claims, where the authentication data include an authentication table.

18. Working method according to claim 17, where the authentication table is generated from a bitstring based on fixed data and variable data.

19. Working method according to claim 18, where variable data comprise any table.

20. Procedure according to claim 19, where the random table is calculated from a random two-dimensional or three-dimensional pattern.

21. Procedure according to claim 1, further comprehensive identification of the user of the electronic device for the activation of the authentication software.

22. Working method according to one of the previous claims, in which the authentication software has a secret encryption key for encrypting digital data.

23. System for executing an electronic transaction between a first transactional party and a second transactional party using an electronic device operated by the first transactional party, where the electronic device has an operating system that creates a run-time environment for user applications:
means for providing authentication information within a storage area of the said electronic device, where the said storage area is a secure part of a Basic In Out System or any other secure location within the said electronic device, which authentication information is inaccessible to a user of the electronic device, where the authentication information is encrypted when the authentication information is stored in the said storage area, where a decryption key for decryption of the authentication data is embedded in the electronic device, where the said decryption key is inaccessible to the said user, to any user-operated software and to the said operating system, where the said memory is inaccessible to the said operating system of the said electronic device, thereby rendering the authentication data inaccessible to the said user,
means for the provision of authentication software in that electronic device, where the authentication data is accessible to that authentication software, where the authentication software is stored in a secure storage location inaccessible to that operating system,

means of activating the authentication software to generate a digital signature from the authentication data, where the authentication software is executed in a secure processing environment inaccessible to the said operating system,
means of providing the digital signature to the second party to the transaction, and
means of providing digital data from the second transaction party to the first transaction party.

24. Electronic device for performing an electronic transaction between a first transaction party and a second transaction party, where the electronic device is operated by the first transaction party, where the electronic device has an operating system that creates a run-time environment for user applications, where the electronic device includes:
a memory that stores authentication information, where said memory is a secure part of a Basic In Out System or any other secure location in said electronic device, which authentication information is inaccessible to a user of the electronic device, where the authentication information is encrypted when the authentication information is stored in said memory, where a decryption key for decryption of the authentication data is embedded in the electronic device, where the said decryption key is inaccessible to the said user, to any user-operated software and to the said operating system, where the said memory is inaccessible to the said operating system of the said electronic device, thereby rendering the authentication data inaccessible to the said user,
a memory that stores authentication software, where the authentication data is accessible to the said authentication software, where the authentication software is stored in a secure memory location inaccessible to the said operating system,
means of activating the authentication software to enable a digital
generate a signature from the authentication data, with the authentication software running in a secure processing environment inaccessible to the said operating system, and
means of providing the digital signature to the second party to the transaction.

25. Electronic device according to claim 24, where the electronic device is a personal computer, a mobile phone, a portable personal digital assistant with wireless communication capabilities, or a device with a BIOS.

2.10. The authentic description of EP 099 describes the following (included where relevant):

**[0002]** At present, numerous transactions are being handled by electronic means in digital format. Digital networks have evolved which enable parties of different kind across the world to communicate with each other and to exchange data and information to reach desired transactions.
**[0003]** The data and information exchanged in said transactions may be legally privileged or protected by copyright, for example. However, digital information may be very easily copied and spread without a trace of who illegally copied and spread the data.

**[0004]** Further, in particular in transactions involving private network access, financial commitments, settlements and/or payments, each party involved in such a transaction wants to identify any other party, or at least, to be able to track any other party, if after completion of the transaction a problem arises. For such identification purposes, it is known to use personal identifiers, such as passwords, Personal Identification Numbers (PIN), and the like, which are only known to a specific user. However, using personal identifiers over public networks like the Internet, there is a possibility that the personal identifier becomes known to another person, enabling this other person to do transactions or gain access to digital data presenting himself as somebody else. If a problem arises after completion of the transaction, it is not possible to track the real transaction partner, as its personal identifier may have been used by a malicious user of the public network.

(…)

**[0007]** A disadvantage of (...) systems employing additional hardware is that the additional hardware, e.g. a token and a token reader, should be supplied to every possible transaction party.

**[0008]** It is therefore an object of the present invention to provide a method and system for performing an electronic transaction or electronic verification or identification without requiring additional hardware.

**[0009]** At least this object is achieved in the present invention by 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 method comprises providing authentication data in a memory of said electronic device, which authentication data are inaccessible to a user of the electronic device; providing authentication software in said electronic device, the authentication data being accessible to said authentication software; activating the authentication software to generate a digital signature from the authentication data; providing the digital signature to the second transaction party. In a preferred embodiment, the second transaction party provides digital data to the first transaction party.

**[0010]** In a further aspect, the present invention provides a method for performing a verification of legitimate use of digital data on an electronic device. The method comprises providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device; providing authentication software in said electronic device, the authentication data being accessible to said authentication software; activating the authentication software to generate a digital signature from the authentication data; providing the digital signature to an application which accesses digital data having a digital signature embedded therein; and comparing the digital signature embedded in the digital data with the provided digital signature.

**[0011]** In another aspect, the present invention provides a method for encrypting digital data on an electronic device using an encryption key, the method comprising gathering session specific data; hashing said session specific data to obtain reference numbers referring to positions in an authorization table stored in said electronic device; generating said encryption key from the characters stored in the authorization table at said positions; and encrypting said digital data using said encryption key.

**[0012]** In a further aspect, the present invention provides systems for performing said methods.

**[0013]** Without use of any additional hardware, a transaction party in an electronic transaction may be identified with virtually no possibility for fraudulent use of the method. In a private network access transaction, the first transaction party is uniquely identifiable by its digital signature. Said digital signature is provided to the second transaction party that

may store the digital signature. If a problem arises later, the first transaction party may be traced and identified by the digital signature provided to the second transaction party.

**[0014]** If digital data are provided to the first transaction party, e.g. copyright protected files such as music and the like, that are digitally signed according to the present invention, i.e. a digital signature is embedded in the digital data, said digital data may be traced, if they are later found to be illegally copied or spread. The embedded digital signature is uniquely traceable to the original first transaction party that received said digitally signed digital data.

**[0015]** Digital data digitally signed according to the present invention are stored in a storage medium of a device having the authentication software installed. The signature has been generated in accordance with the authentication data stored in said device and thereafter embedded in the digital data to protect the data and to be able to trace a malicious user.

[**0016]** The signature embedded in the data may also be employed to prevent that the data are illegally used, since the signature may be regenerated by the device at any time. As a regenerated signature should be identical to the one embedded in the digital data, a comparison of the embedded signature with the regenerated signature provides information whether the digital data is rightfully installed on the device. If the comparison shows that the signatures are identical, the data may be accessed by the device, and, for example, an application comprised in said digital.data may be run or said digital data may be accessed by any other application, for example for playing music represented by said digital data. When the signatures are not identical, the digital data are illegally installed, e.g. copied from another device, and they may not be accessed and read by the device and an error signal may be generated.'

2.11. EP 099 contains, inter alia, the following figures:

Figuur 1

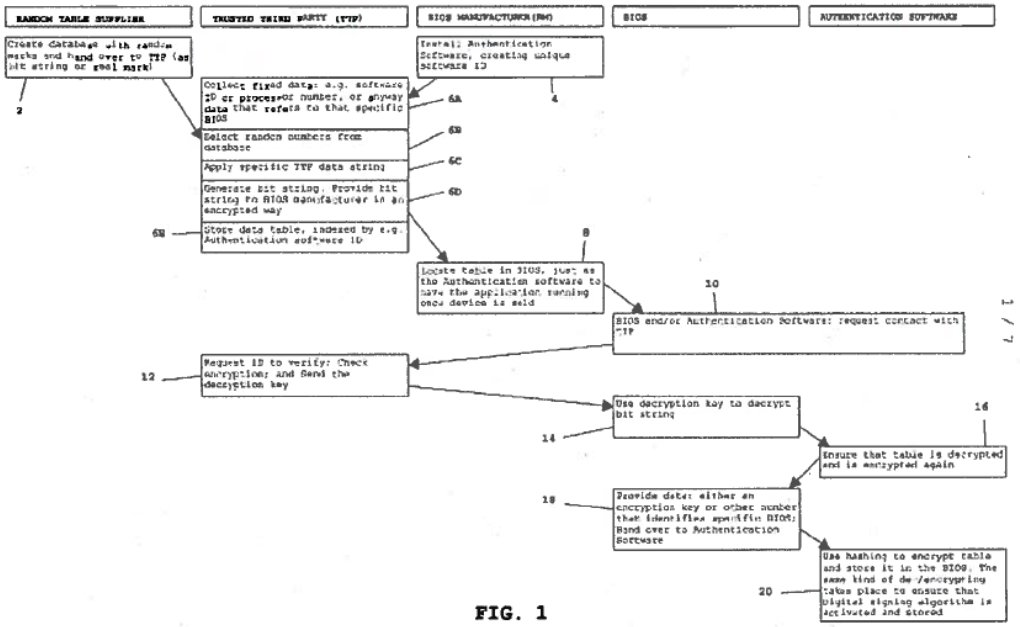


FIG. 1

Figuur 2

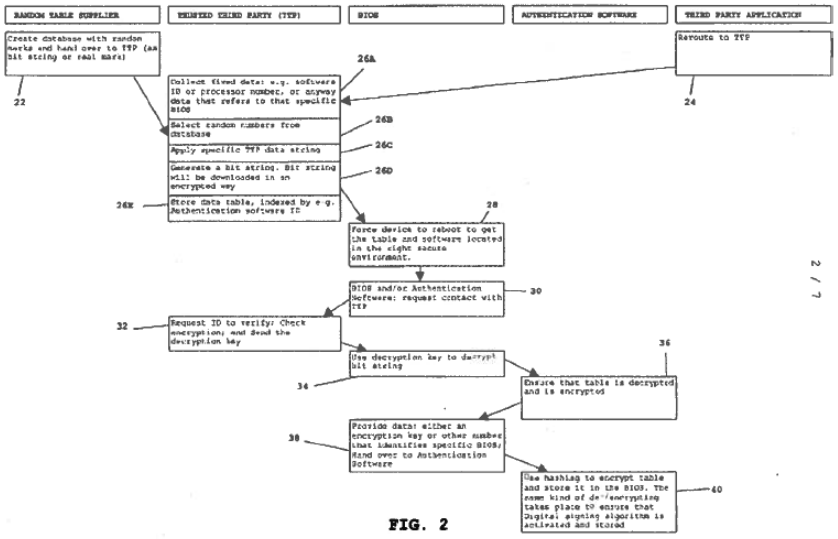


FIG. 2

2 / 7

Figuur 3

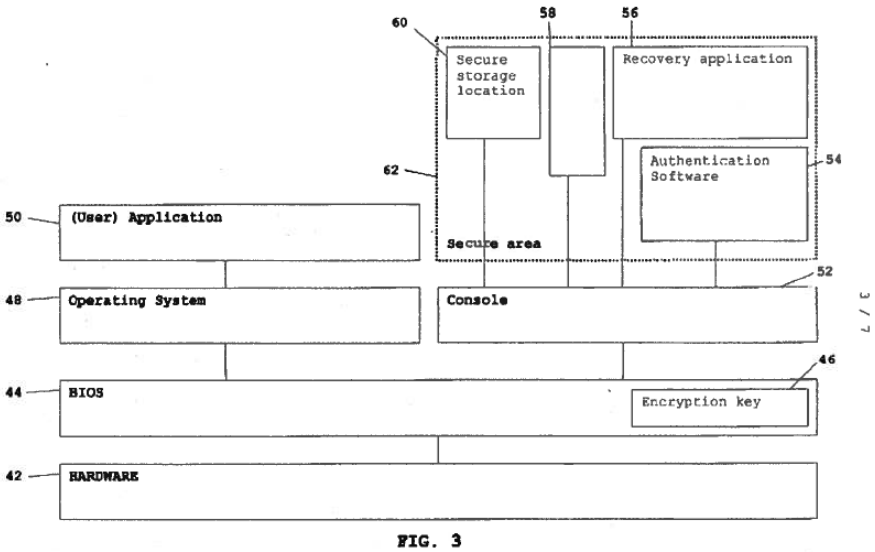


FIG. 3

3 / 7

Figuur 5A en 5B

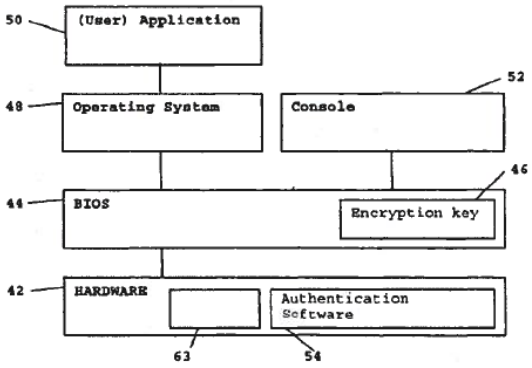


FIG. 5A

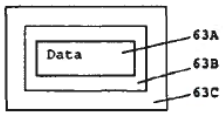


FIG. 5B

2.12 EP 140, like EP 099, contains an independent method claim (Claim 1) and 21 claims dependent on that claim, an independent system claim (Claim 23), an independent product claim (Claim 24) and one claim dependent on that product claim (claim 25).

2.13. The claims of EP 140, in the authentic English version, are as follows:

1. 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 (48) creating a run-time environment for user applications and authentication software (54) running in a separate operating environment, independent from and inaccessible to said operating system, (48) the electronic device having a memory comprising storage locations, part of the memory being accessible to the operating system, (48) part of the memory being a secure area (62) storage locations of which are not reported to the operating system, (48) the method comprising:
providing authentication data (63A) in the secure area (62) of said electronic device which authentication data (63A) are inaccessible to a user of said electronic device, wherein said secure area (62) is inaccessible to said operating system (48) of said electronic device, thereby rendering the authentication data (63A) inaccessible to said user;
providing authentication software (54) in said electronic device, the authentication data (63A) being accessible to said authentication software, (54) wherein the authentication software (54) is stored in the secure area (62) inaccessible to said operating system (48)
activating the authentication software (54) to generate a digital signature from the authentication data, (63A) wherein the authentication software (54) is run in a secure processing environment inaccessible to said operating system (48) providing the digital

signature to the second transaction party.

2. Method according to any of the preceding claims, wherein the authentication data are provided by the second transaction party, which stores the authentication data together with data identifying the first transaction party.

3. Method according to claim 2, wherein the second transaction party uses the stored authentication data to obtain transaction specific authentication data according to a specific algorithm.

4. Method according to claim 3, wherein the second transaction party verifies the digital signature provided by the first transaction party using the authentication data stored at the second transaction party.

5. Method according to claim 1, wherein the authentication software has its own unique serial number, software ID and/or private encryption key.

6. Method according to any of the preceding claims, wherein the authentication data are encrypted by the second transaction party using an encryption key before the authentication data are provided to the first transaction party.

7. Method according to claim 6, wherein the authentication software retrieves a decryption key associated with the encryption key and decrypts the authentication data at its first use.

8. Method according to claim 1, wherein the authentication software is installed in an application environment in the secure area such that it may obtain the authentication data without passing through an unsecured part of said electronic device.

9. Method according to claim 1, wherein the authentication data, and the authentication software including the digital signing algorithm are locked in the secure area.

10. Method according to any of the preceding claims, wherein the authentication data are encrypted, when the authentication data are stored in said secure area, a decryption key for decrypting the authentication data being inaccessible to said user and to any user- operated software, thereby rendering the authentication data inaccessible to said user.

11. Method as in any one of the preceding claims, wherein the authentication software is executed to initiate decryption of the authentication data stored in the secure area for generating said digital signature.

12. Method according to any of the preceding claims, wherein the authentication data are encrypted using at least two encryption layers.

13. Method according to any of the preceding claims, wherein the authentication data are encrypted using an encryption key which is associated with a hardware device serial number.

14. Method according to any of the preceding claims, wherein the authentication data are encrypted using an encryption key which is associated with a user identifying number, in

particular a personal identifying number, PIN, or a number or a template associated with a fingerprint of the user, or the like.

15. Method according to claim 12, wherein at least one encryption layer is decryptable using a decryption key associated with one or more serial numbers of hardware components of said electronic device.

16. Method according to any of the preceding claims, wherein at least one encryption layer may be decrypted by the authentication software.

17. Method according to any of the preceding claims, wherein another encryption layer is an encryption/decryption application stored in the electronic device using a device specific encryption key.

18. Method according to claim 17, wherein the encryption/decryption application is stored in a Basic Input-Output System, BIOS, or in a secure area.

19. Method according to claim 12, wherein a second encryption layer is decrypted using a decryption key associated with any identifying characteristic, in particular a serial number, a personal identification number, PIN, or a fingerprint of a user.

20. Method according to any of claims 14 to 19, wherein the authentication data are decrypted in a secure processing environment inaccessible to said user and to any user-operated software.

21. Method according to claim 1, further comprising identifying the user of the electronic device before activating the authentication software.

22. Method according to any one of the preceding claims, wherein the authentication software has a private encryption key for encrypting digital data.

23. System 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 said 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 storage locations of which are not reported to the operating system, the system comprising:
means for providing authentication data in the secure area of said electronic device which authentication data are inaccessible to a user of the electronic device, wherein said secure area is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;
means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software, wherein the authentication software is stored in the secure area inaccessible to said operating system;
means for activating the authentication software to generate a digital signature from the authentication data, wherein the authentication software is run in a secure processing environment inaccessible to said operating system;

means for providing the digital signature to the second transaction party.

24. Electronic device for performing an electronic transaction between a first transaction party and a second transaction party, wherein the electronic device is 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 said 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 storage locations of which are not reported to the operating system,
the secure area storing authentication data which are inaccessible to a user of the electronic device, wherein said secure area is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user; the electronic device comprising:
a memory storing authentication software, the authentication data being accessible to said authentication software, wherein the authentication software is stored in the secure area inaccessible to said operating system;
means for activating the authentication software to generate a digital signature from the authentication data, wherein the authentication software is run in a secure processing environment inaccessible to said operating system; and
means for providing the digital signature to the second transaction party.

25. Electronic device according to claim 24, wherein the electronic device is a personal computer, a cellular phone, a hand-held personal digital assistant with wireless communication capabilities, or a device containing a BIOS.

2.14. In the (undisputed) Dutch translation, the claims of EP 140 are as follows:

1. Procedure for executing an electronic transaction between a first transactional party and a second transactional party using an electronic device operated by the first transactional party, where the electronic device has an operating system (48) that creates a run-time environment for user applications, and authentication software (54) that runs in a separate execution environment, independent of and inaccessible to the said operating system (48), where the electronic device has a storage location, where part of the storage is accessible to the operating system (48), where part of the storage is a secure area (62), where storage locations are not reported to the operating system (48), where the operating mode includes operation:
provision of authentication information in the secure area of said
electronic device, which authentication information is inaccessible to a user of the said electronic device, where the said secure area is inaccessible to the said operating system of the said electronic device, making the authentication information inaccessible to the said user; provision of authentication software in the said electronic device, where the authentication information is accessible to the said authentication software, where the authentication software is stored in the secure area inaccessible to the said operating system;
activate the authentication software to generate a digital signature from

the authentication data, where the authentication software is executed in a secure processing environment inaccessible to the said operating system; provision of the digital signature to the second transaction party.

2. Procedure according to one of the above claims, where the authentication data are provided by the second transaction party, who stores the authentication data together with data identifying the first transaction party.

3. Working method according to claim 2, where the second transaction party uses the stored authentication data to obtain transaction-specific authentication data according to a specific algorithm.

4. Working method according to claim 3, in which the second transaction party verifies the digital signature provided by the first transaction party using the authentication data stored with the second transaction party.

5. Procedure according to claim 1, whereby the authentication software has its own unique serial number, software ID and/or private encryption key.

6. Operation according to one of the previous claims, whereby the authentication data are encrypted by the second transaction party using an encryption key before the authentication data are provided to the first transaction party.

7. Working method according to claim 6, in which the authentication software retrieves a decryption key associated with the encryption key and decrypts the authentication data when they are first used.
8. Procedure according to Claim 1, whereby the authentication software is installed in an application environment in the secure area in such a way that it can obtain the authentication data without going through an unsecured part of the said electronic device.

9. Working method according to claim 1, in which the authentication data and the authentication software including the digital signature algorithm are locked in the secure area.

24. Operation in accordance with one of the foregoing claims, whereby the authentication data are encrypted when the authentication data are stored in the said secure area, whereby a decryption key for decryption of the authentication data is inaccessible to the said user and to any user-operated software, thereby rendering the authentication data inaccessible to the said user.

25. Operation in accordance with one of the above claims, whereby the authentication software is executed to start decryption of the authentication data stored in the secure area for the generation of the said digital signature.

26. Procedure according to one of the previous claims, whereby the authentication data is encrypted with at least two layers of encryption.

13. Procedure according to one of the previous claims, where the authentication data is encrypted with an encryption key associated with a hardware device serial number.

14. Operation according to one of the above claims, whereby the authentication data are encrypted with an encryption key associated with a user identification number, in particular a personal identification number, PIN, or a number or template associated with a fingerprint of the user, or similar.

15. Procedure according to Claim 12, whereby at least one layer of encryption is decrypted using a decryption key associated with one or more serial numbers of hardware components of the said electronic device.

16. Procedure according to one of the previous claims, whereby at least one layer of encryption can be decrypted by the authentication software.

17. Procedure according to one of the previous claims, where another layer of encryption is an encryption/decryption application stored in the electronic device with a device-specific encryption key.

18. Procedure according to claim 17, where the encryption/decryption application is stored in a Basic Input-Output System, BIOS, or in a secure area.

19. Procedure according to Claim 12, whereby a second layer of encryption is decrypted using a decryption key associated with any identifying characteristic, in particular a serial number, a personal identification number, PIN, or a fingerprint of a user.

20. Operation according to one of claims 14 to 19, whereby the authentication data are decrypted in a secure processing environment inaccessible to the said user and to any user-operated software.

21. Procedure according to claim 1, further comprehensive identification of the user of the electronic device for activation of the authentication software.

22. Procedure according to one of the previous claims, whereby the authentication software has a private encryption key for encrypting digital data.

23. System for executing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, where the electronic device has an operating system that creates a run-time environment for user applications, and authentication software that runs in a separate execution environment, independent of and inaccessible to that operating system, where the electronic device has memory that includes storage locations, where part of memory is accessible to the operating system, where part of memory is a secure area, where storage locations are not reported to the operating system, where the system includes storage locations:
means for the provision of authentication data in the secure area of

said electronic device, which authentication information is inaccessible to a user of the electronic device, where the said secure area is inaccessible to the said operating system of the said electronic device, rendering the authentication information inaccessible to the said user;
means for providing authentication software in that electronic device, where the authentication data is accessible to that authentication software, where the authentication software is stored in the secure area inaccessible to that operating system;
means of activating the authentication software to generate a digital signature from the authentication data, where the authentication software is executed in a secure processing environment inaccessible to the said operating system;
means of providing the digital signature to the second party to the transaction.

24. Electronic device for executing an electronic transaction between a first transaction party and a second transaction party, where the electronic device is operated by the first transaction party, where the electronic device has an operating system that creates a run-time environment for user applications, and authentication software that runs in a separate execution environment, independent of and inaccessible to the said operating system, where the electronic device has a memory that includes storage locations, where part of the memory is accessible to the operating system, where part of the memory is a secure area, where storage locations are not reported to the operating system,
where the secure area stores authentication information that is inaccessible to a user of the said electronic device, where the secure area is inaccessible to the operating system of the said electronic device, thereby rendering the authentication information inaccessible to the said user; where the electronic device includes:
a memory that stores authentication software, where the authentication data is accessible to the said authentication software, where the authentication software is stored in the secure area inaccessible to the said operating system; means for activating the authentication software to generate a digital signature from the authentication data, where the authentication software is run in a secure processing environment inaccessible to the said operating system; and
means of providing the digital signature to the second party to the transaction.

25. Electronic device according to claim 24, where the electronic device is a personal computer, a mobile phone, a portable personal digital assistant with wireless communication capabilities, or a device with a BIOS.

2.15. The extracts from the description of EP 099 quoted above under 2.10 are also included in par. [0002] to [0015] of the description of EP 140. EP 140 also includes the figures shown in 2.11.

*WO 752*

2.16. The description of WO 752 discloses what has been set out above in 2.10 and 2.11 from the description and figures of EP 099, as well as the following (from page 4):

> The invention and its aspects, features, and advantages will be more readily appreciated as the same becomes better understood by reference to the following detailed description and considered in connection with the accompanying drawings provided by way of non-limiting examples, in which drawings like reference symbols designate like actions or parts.
>
> Fig. 1 illustrates a chart of an installation method for a new device according to the present invention.
>
> Fig. 2 illustrates a chart of an installation method for an existing device according to the present invention.
>
> Fig. 3 schematically illustrates a computer configuration having authentication software and an authentication table installed in the BIOS according to the present invention.
>
> Fig. 4 illustrates a chart of another installation method for an existing device according to the present invention.

page 5:

> In this context, an installation method is to be understood as a method for installing software at some actors involved in the present method for enabling tracking and tracing of at least one transaction party. Further in this context, a new device relates to any electronic device containing a Basic In Out System ("BIOS", "Boot agent" etc.) with any associated secure storage/memory location, e.g. a computer, seDCCPer, printer, personal digital

page 6:

assistant, mobile telephone, which is being manufactured, or has been manufactured, but has not yet been delivered to an end-user, whereas an existing device relates to any electronic device containing a Basic In Out System which has been delivered to an end-user, and may or may not have been used by the end-user. The Basic In Out System is only referred to as a system for accessing a memory location in a memory that is directly or indirectly connected to the electronic device. However, as is described hereinafter, the method according to the present invention may employ such a BIOS system to securely store certain digital data and/or such a BIOS system may be provided with an encryption system. A secure storage location and/or an encryption system are not essential to the BIOS system with respect to the present invention.

Fig. 1 illustrates a first preferred embodiment of the present invention. Referring to Fig. 1, an installation method for a new device is illustrated. The method of Fig. 1 includes five actors: a random table supplier, a trusted third party, a BIOS manufacturer, a BIOS and authentication software. The first, second and third actors are physical entities, e.g. persons or companies, whereas the fourth and fifth actors are software embedded in a device.

page 7:

The BIOS which is supplied by the BIOS manufacturer, is also an actor in the method, and its actions are represented by the fourth column of Fig. 1. The BIOS may be coupled to the TTP to receive a decryption code and enable the authentication software to decrypt an authentication table, which will then be encoded again and stored in a secure part of the device, only accessible to the BIOS.

The fifth column of Fig. 1 represents the actions of the authentication software, which may be supplied by the random table supplier or by any other third party and is stored in the BIOS. The authentication software may be coupled to the TTP to decrypt the bit string in the BIOS into an authentication table, encrypts the authentication table again and stores it in the secure part of the device, only accessible to the BIOS. Further, the authentication software stores and activates a digital-signing algorithm to generate a session- or transaction-specific digital signature. The a.7_hentication software preferably runs in a separate operating environment in the BIOS or in a console and is independent from and Inaccessible to the operating system (OS; on the device.

page 8:

According to cell 4, a BIOS manufacturer embeds or installs authentication software in the BIOS. The authentication software **may** be supplied by the random table supplier, generated *by* the BIOS manufacturer or supplied by a third party.

page 10:

The installation in a new device is completed according to cell 20. The encoded authentication table is stored in a secure part of the BIOS, where it may only be retrieved by the BIOS and not by the operating system. This secure part of the BIOS may also be any other secure location in the device. For instance, it may be a separate part of a hard drive of a computer, which part may not be accessible to the operating system, but only to the BIOS and/or authentication software. Storing the authentication table in a secure location further decreases the possibility of retrieval of the authentication table .

The device is now set-up. Authentication software and an encoded authentication table are installed in the BIOS. Further, in a database of a trusted third party (TTP), data are stored which enable the TTP to generate the same authentication table *when* later needed.

Fig. 2 illustrates a second preferred embodiment. In the second preferred embodiment, the installation method is performed on an

page 11:

existing computer device. The existing device does not have authentication software installed in its BIOS, nor does it have an encrypted bit string stored in its BIOS at the time a digital signature according to the present invention is needed *for* any track and trace purpose, including a particular electronic session, e.g. a network access procedure, or an on-line transaction. Thus, compared to a new computer device, further steps are necessary in the above-described installation method to install the necessary software and authentication table in a secure memory location of the *device.* Such a secure memory location may be a part of a secure memory or it may be an encrypted part of a non-secure memory, such as a user-accessible memory.

page 12:

The authentication software and the bit string are put in a part of the BIOS which **is** accessible to the operating system according to cell 26A. Next, according to cell 28B, the device needs to reboot to store the authentication software and the bit string in a secure part of the BIOS which is not accessible for the operating system.

page 13:

Fig. 3 schematically illustrates a possible configuration of a device having the authentication software and an' authentication table installed. The device consists of several components, commonly referred to as hardware 42. Exemplary hardware components are a processor, a hard drive, or other memory and a keyboard. All the hardware devices are controlled by the BIOS 44. The BIOS 44 is a software package stored in a read-only memory (ROMI, usually located on a main board, which is one of the hardware components of an electronic device.

The BIOS 44 controls most of the instructions and data flowing from one component to another. Data or instructions coming from one component and addressed to another need to pass through the BIOS 44. The BIOS 44 may check whether the instructions to the other component are allowed or not, as not every component is accessible for any other component. The BIOS 44 may comprise an encryption key 46. Such an encryption key 46 may be used to encrypt data and only another party who mows the encryption key 46 ***may be*** able to decrypt the data.

The operating system 48 creates a run-time environment for any user applications. Therefore, it may be stated that the operating system 48 is an interface between a user and the hardware 42. A user may instruct the operating system 48 to run an application 50. If the application 50 needs data that are stored on the hard drive, the application 50 requests the data from the operating system 48. The operating system 48 in turn requests the data through the BIOS 44 from the hardware 42, i.e. the hard drive. The data coming from the hardware 42 pass through the BIOS 44 and the operating system 08 before they arrive at the requesting application 50. Via this protocol the BIOS 44 may control the accessibility of certain data or hardware devices 42 and thus the use of particular software. It may prohibit, for example, the operating system 48 to access certain pasts of a hard drive or start certain applications.

page 14:

A console 52 is an environment, which runs all the processes in computer without user interruption. The console 52 plays an important role at start-up of the computer, instructing the hardware devices 42 via the BIOS 44 to start and report their status. In case of *errors,* not only at start-up but also during operation, the BIOS 44 sends toe error massages coming from the hardware 42 to the console 52. The console 52 then handles and corrects the errors. Thus, the console 52 runs more or less stand-alone the computer. A user may not interrupt or influence the console 52. Any instructions coming from the operating system 4e intended for the console 52 nay therefore be blocked.by the BIOS 44.

In or behind the console 52, there 13 a secure area 62 only accessible to the BIOS. The secure area 62 comprises applications and storage locations, which are not reported to the operating system 48. That means that the operating system 48 does not know that the applications and data in the storage locations are present and maybe even running in a separate environment. For example, when a hardware device 42 reports an error, the console 52 may run a recovery application 56 to handle the error such that the hardware device 42 recovers from the error and is able to continue its operation. The operating system 48 has probably not even noticed that there was an error.

An authentication table may be securely stored in the secure storage location 60. In such a part of the computer, commonly seen 75 as a part of the BIOS 44, the authentication table is unreachable *for* the operating system 48 and thus for a user.

With the authentication table securely stored in the secure storage location 60, the authentication software 54 should run in an environment in the BIOS 44, thus preventing that the authentication table is accessible to *the* operating system 48 at any time. Therefore, the authentication software 54 may be installed .n an application environment in the secure area 67 such that it may obtain the authentication table without passing through an unsecured part of the device.

page 15:

In a third preferred installation method illustrated in Fig. 4, the authentication data, e.g. authentication table, is stored in a memory that is accessible to an operating system of the device and possibly to a user *of* said device. To prevent that the user may obtain the authentication data, which should be prevented as described above, the authentication data are encrypted. Thus, the user may only obtain encrypted authentication data. To prevent that the authentication data becomes accessible to a user, the authentication data should only be decrypted in a secure processing environment such as a 'Ring Pero' processing environment, which is embedded in a processing unit of commonly used personal computers. Such a secure processing environment may only be accessible to selected software applications, preferably not to user-operated software applications. Further, a decryption algorithm and/or a decryption key should not be obtainable to any user.

2.17. The authentic text of the claims of WO 752 reads as follows:

1. 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 method comprising: providing authentication data in a memory of said electronic device

which authentication data are inaccessible to a user of said electronic device; providing authentication software in said electronic device, the authentication data being accessible to

2. Method according to claim 1, wherein the second transaction party provides digital data to the first transaction party.

3. Method according to claim 2, wherein the second transaction party embeds the digital signature in the digital data provided to the first transaction party.

4. Method according to claim 1,2 or 3, wherein the second transaction party stores the digital signature together with data identifying the first transaction party.

5. Method according to any of the preceding claims, wherein the authentication data are provided by the second transaction party, which stores the authentication data together wi-th data identifying the first transaction party.

6. Method according to claim 5, wherein the second transaction party uses the stored authentication data to obtain transaction specific authentication data according to a specific algorithm.

7. Method according to claim 6, wherein the second transaction party verifies the digital signature provided by the first transaction party using the authentication data stored at the second transaction party.

8. Method according to any of the preceding claims, wherein the first transaction party further provides a signed digital signature to the second transaction party, the signed digital signature being generated by the authentication software by signing the digital signature using a private key, which private key is unique for said authentication software and is known to a third party.

9. Method for performing a verification of legitimate use of digital data on an electronic device, the method comprising: providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device; providing authentication software in said electronic device, the authentication data being accessible to said authentication software ; activating the authentication software to regenerate a digital signature from the authentication data; providing the digital signature to the authentication software by an application accessing digital data having a digital signature embedded therein; and comparing the regenerated digital signature with the embedded digital signature.

10. Method according to any of the preceding claims, wherein the authentication data are encrypted by the second transaction party using an encryption key before the authentication data are provided to the first transaction party.

11. Method according to claim 10, wherein the authentication software retrieves a decryption key associated with the encryption key and decrypts the authentication data at its first use.

12. Method according to any of the preceding claims, wherein said memory is inaccessible to an operating system of said electronic device, thereby rendering the authentication data inaccessible to said user.

13. Method according to claim 12, wherein the authentication data are provided in a Basic Input-Output System (BIOS) of the electronic device.

14. Method according to any of the preceding claims, wherein the authentication data are encrypted, when the authentication data are stored in said memory, a decryption key for decrypting. the authentication data being inaccessible to said user and to any user-operated software, thereby rendering the authentication data inaccessible to said user.

15. Method according to claim 14, wherein the authentication data are encrypted using at least two encryption layers.

16. Method according to claim 15, wherein at least one encryption layer may be decrypted using a decryption key associated with one or more serial numbers of hardware components of said electronic device.

17. Method according to claim 15 or 16, wherein at least one encryption layer may be decrypted by the authentication software.

18. Method according to any of claims 14-17, wherein the authentication data are decrypted in a secure processing, environment inaccessible to said user and to any user-operated software.

19. Method according to any of the preceding claims, wherein the authentication data comprise an authentication table.

20. Method according to claim 19, wherein the authentication table is generated from a bit string which is generated from fixed data and variable data.

21. Method according to claim 20, wherein the fixed data are at least part of a serial number of a hardware device.

22. Method according to claim 20, wherein the fixed data are at least part of a device specific software identification code of the authentication software.

23. Method according to claim 20,21 or 22, wherein the variable data comprise a random table.

24. Method according to claim 23, wherein the random table is calculated from a random two-dimensional or three-dimensional pattern.

25. Method according to any of claims 19-24, wherein the authentication table is generated from fixed data, variable data and a bit string, which bit string is specific to a trusted third party that provides the authentication data.

26. Method according to any of the preceding claims, wherein the authentication software is

stored in a secure memory location inaccessible to an operating system.

27. Method according to any of the preceding claims, wherein the authentication software is run in a secure processing environment inaccessible to an operating system.

28. Method for encrypting digital data on an electronic device using an encryption key, the method comprising: gathering session specific data; hashing said session specific data to obtain reference numbers referring to positions in an authentication table stored in said electronic device; generating said encryption key from the characters stored in the authentication table at said positions; and encrypting said digital data using said encryption key.

29. System for performing an electronic transaction between a first transaction party and a second transaction using an electronic device operated by the first transaction party, the system comprising: means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device; means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software; means for activating the authentication software to generate a digital signature from the authentication data; means for providing the digital signature to the second transaction party; and means for providing digital data from the second transaction party to the first transaction party.

30. System for performing a verification of legitimate use of digital data on an electronic device, the system comprising: means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device; means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software;
means for activating the authentication software to generate a digital signature from the authentication data; means for providing the digital signature to the authentication software by an application accessing digital data having a digital signature embedded therein; and means for comparing the regenerated digital signature with the embedded digital signature.

31. System for encrypting digital data using an encryption key, the system comprising: means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device; means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software; means for activating the authentication software to generate a digital signature from the authentication data; means for gathering session specific data ; means for hashing said session specific data to obtain reference numbers referring to positions in an authentication table stored in said electronic device; means for generating said encryption key from the characters stored in the authorization table at said positions; and means for encrypting said digital data using said encryption key.

2.18. Figures 1, 2 and 3 shown in 2.11 are also shown, with the same numbering, in WO 752.

## 3. The dispute in both cases

**in the main action**

3.1. DTS claims - in summary - that the court, as far as possible provisionally enforceable:
- prohibits Samsung c.s. to infringe EP 099 and EP 140 in the Netherlands and the other designated countries;
- orders Samsung c.s. to recall products, to destroy the infringing products held in stock and recalled, to compensate DTS for the damages suffered and to be suffered or to pay the profits made, and to provide details of the manufacturer, suppliers and commercial customers of the infringing products as well as details relevant for the calculation of compensation/profit;
- orders Samsung c.s. to pay the costs of the proceedings pursuant to Article 1019h DCC.

3.2. Underlying these claims is the fact that the functionality of all Samsung c.s. mobile phones, tablets and smartwatches in the Netherlands and in the other designed countries - in brief - are covered by the scope of protection of independent claims 1, 23 and 24 and dependent claims 2, 5 to 8, 11, 13 to 16, 21, 22 and 25 of EP 099 and by the scope of protection of independent claims 1, 23 and 24 and dependent claims 2, 5 to 11, 14, 16 to 18, 20 to 22 and 25 of EP 140 and Samsung c.s. thus infringes, directly or indirectly, EP 099 and EP 140.

3.3. Samsung c.s. put forward a reasoned defence rejecting the claims of DTS, ordering DTS to pay the costs of the proceedings under Article 1019h DCC.[2] Samsung c.s. primarily argues that EP 099 is invalid because of (i) added matter within the meaning of Article 75 (1)(c) of the DPA[3] and Article 123(2) in conjunction with Article 138(1)(c) EPC,[4] (ii) lack of sufficiency, (iii) lack of novelty (in view of the relevant prior art) and (iv) lack of inventive step (in view of the relevant prior art and partly because the priority invoked is not valid). In the alternative, Samsung c.s. argues that, should EP 099 be considered valid, there is no (direct and indirect) infringement.

3.4. Samsung c.s. primarily raises the same validity objections to EP 140 as to EP 099, with the exception of the objection that the patent lacks sufficiency. In the alternative, Samsung c.s. argues, just as in the case regarding EP 099, that, if the patent is valid, Samsung c.s. does not (directly or indirectly) infringe.

**in the counterclaim action**

3.5. Samsung c.s. claims in the counterclaim action that the court by judgment, as far as possible provisionally enforceable, invalidates the Dutch part of EP 099 and the Dutch part of EP 140 and orders DTS to pay the costs of the proceedings pursuant to Article 1019h DCC.

[2] the Dutch Code of Civil Procedure (DCC)
[3] The Dutch Patent Act (DPA)
[4] European Patent Convention (EPC)

3.6. These claims are based on the fact that EP 099 and EP 140 are invalid for the reasons set out in points 3.3 and 3.4 above.

3.7 DTS puts forward a reasoned defence, resulting in a request for rejection of the claims of Samsung c.s., and to order Samsung c.s. jointly and severally to pay the costs of the proceedings pursuant to Article 1019h DCC.

**4. Technical Background**

4.1. The following technical introduction is derived from the documents of the parties and is not in dispute between them. It is debatable whether all this was already common general knowledge of the relevant skilled person on the priority date.

Computer hardware and software

4.1.1. Each computer has different hardware and software components. The hardware usually includes a central processing unit or CPU, various (volatile and non-volatile) memory components and peripherals, such as a keyboard, mouse, graphics card and so on. Software consists of a set of instructions or code that is executed by the CPU. Examples of software are the BIOS (Basic Input/Output System), an operating system and applications.

Operating system and kernel

4.1.2. The operating system of a computer controls the hardware (including peripherals) and is the intermediary between the computer hardware and application software. The operating system also provides the user interface, through which users can communicate directly with the operating system.

4.1.3. An operating system consists of several components, including a kernel. A kernel is the central part of an operating system, which allows applications to access the hardware, such as the CPU, the computer's working memory (RAM or Random Access Memory, a volatile memory component), but also non-volatile components, such as EEPROM or Flash memory, hard disks and the Input/Output peripherals, such as mouse, keyboard, network, etc. For example, the kernel controls which applications have access to the CPU at which moment, it can make memory available to applications and handles interrupts. Interrupts are signals from hardware and software for notification or request of e.g. CPU access. The kernel also 'translates' input/output requests (`requests') from software into 'data-processing' instructions for a processor chip, e.g. a microprocessor or a CPU.

Basic Input/Output System (BIOS)

4.1.4. The BIOS is software that is - on the priority date of the patents according to DTS: *always* - stored on a non-volatile and non-mutable memory component, a ROM memory. The BIOS is the first piece of software that is loaded when the computer boots and it takes care of, among other things, the identification and configuration of the computer hardware so that the computer can actually function after booting. The

BIOS also takes care of loading the boot loader through the CPU, which then initializes the operating system. In the past (in the MS-DOS era) the BIOS had a function even after the computer was booted and was an intermediary between the CPU and input/output peripherals. In computers with modern operating systems, the BIOS only has a function during computer boot.

Execution of data by the CPU

4.1.5. To process data, the CPU of a computer shall have a working memory, also known as primary memory or internal memory. Software (instructions) and the data on which those instructions are to be executed shall be loaded into that volatile memory so that they can be easily and quickly accessed by the CPU. At the moment that certain software and data are to be executed, they are loaded (by the operating system run by the CPU) from the secondary memory, such as Flash, hard disk or SSD (Solid State Drive), non-volatile memory where those software and data are permanently stored. After being loaded into the primary memory and executed by the CPU, the software and data are erased from the working memory.

**5. The assessment in both cases**

**in the main and counterclaim action**

*Jurisdiction*

5.1. The District Court has international jurisdiction to hear the claims in the main action under Article 4.1 Brussels I bis Regulation[5] because Samsung Electronics Benelux, Samsung Electronics Europe and Samsung Electronics Overseas are domiciled in the Netherlands. The international jurisdiction to take cognizance of the counterclaims seeking to have the Dutch part of EP 099 invalidated and to have the Dutch part of EP 140 invalidated can be based on Article 24 preamble and under (4) of the Brussels I bis Regulation. The relative jurisdiction of this court is based on Article 80(1)(a) DPA 1995.[6]

*Confidentiality regime*

5.2 Samsung c.s. requested the application of a confidentiality regime under Article 1019ib DCC and alternatively under Articles 27 to 29 DCC with respect to certain information provided in its procedural documents and during the hearings in both cases in support of its non-infringement defence. DTS objected to the application of those regimes.

5.3. Since the present cases do not relate to the protection of a business secret, Article 1019ib DCC is not applicable.

[5] Regulation (EU) 1215.2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters
[6] Dutch Patent Act 1995.

5.4. Samsung c.s. have specifically requested the application of Articles 27 to 29 DCC for a number of exhibits (GP32 and 33 in Case I and GP29 and 30 in Case II) and for some parts of the oral argument. This concerns data on the design of the Samsung telephones at issue. DTS's objection that Samsung c.s.'s request is far too general is not valid with respect to the above exhibits. DTS did not reiterate its objection with regard to those specific exhibits after they had been submitted by Samsung c.s.. DTS also does not dispute Samsung c.s.'s significant interest in the confidentiality of data relating to the architecture of Samsung products' security, authentication and verification functions. In view of this, the Court holds that the data in exhibits GP32 and 33 in Case I and GP29 and 30 in Case II are subject to a disclosure restriction under Article 29(1)(b).

5.5 At the hearing in Case II, which was open to the public, part of the oral argument was heard in camera with the consent of both parties (marginal 41 and 42 of the DTS pleading, marginal 31 of the Samsung c.s.' pleading and the parties' explanations). In accordance with Article 27 in conjunction with Article 29 paragraph 1 sub a of the DCC, a prohibition of disclosure also applies to what has been discussed in camera.

5.6. As this judgment does not contain any information deemed confidential by Samsung c.s., the request to apply Article 28 DCC to this judgment is rejected for lack of interest. The judgment as a whole may be pronounced in public.

*Added matter?*

5.7. The Court sees reason to first consider the validity of EP 099 and EP 140. Samsung c.s. disputes the validity of these patents with different arguments. One of these is that the subject matter of EP 099 and EP 140, more specifically that of a number of features common to the independent method claims, the independent system claims and the independent product claims of those patents, was inadmissibly extended during the granting procedure.

5.8. Inadmissible added matter in a claim is deemed to exist if the average person skilled in the art, who makes use of his common general knowledge, is confronted with information in a claim that he cannot directly and unambiguously, explicitly or implicitly, infer from the originally filed application. In answering the question whether such a situation exists, the originally filed application must be considered as a whole. Consideration must be given to the claims, the description and the drawings. This is referred to in the *case law of the* Boards of Appeal of the EPO as the 'disclosure test' or ‘gold standard'. The reason for this validity objection is that the applicant of the patent may not improve his legal position by claiming protection for matter that was not disclosed in the original application. After all, the legal certainty of third parties may be compromised as a result.

5.9. The *case law of* the EPO distinguishes between various categories of cases in which the claims amended during the granting procedure do not find a basis in the original application. One of the categories developed by the EPO

is the intermediate generalisation. In that case, in an amended (granted) claim, a feature of a particular embodiment or disclosure is selectively omitted or generalised outside the originally disclosed context. Modifying a claim by including a technical feature that has only been disclosed in conjunction with other features is, in the *case law of* the EPO, only permitted if there is no structural or functional (i.e. inseparable) link between those features described in combination. In line with G 2/10[7], the court is of the opinion that this *case law* is only an aid and that ultimately only the answer to the previously formulated main question (the 'gold standard') is decisive.[8]

5.10 WO 752 qualifies to both EP 099 and EP 140 as the original application.

5.11. The parties agree that the skilled person is a 'computer scientist' with knowledge and skills of (mobile) computer systems and electronic transactions and with several years of experience in the development of hardware and software for carrying out secure electronic transactions. According to Samsung c.s. the average person skilled in the art also has to be an expert in the field of cryptography, which is disputed by DTS. The District Court is of the opinion that, in view of the subject matter of EP 099 and EP 140, the average person skilled in the art does not need to have knowledge of cryptography. The problem that the patents identify concerns the security, authentication and verification of electronic transactions without the need for additional hardware, such as token readers (compare [0007] of EP 099 and [0006] of EP 140). This does not require substantive knowledge of encryption and decryption methods, at most understanding of the associated data flows.

5.12. The District Court also notes that the common general knowledge that the average person skilled in the art will use is the common general knowledge on 13 June 2003, the priority date invoked in the application for EP 099 and EP 140.

*EP 099*

5.13. According to the parties, the independent method claim 1 consists of fifteen distinguishable features. The District Court will also take this classification as a starting point. In the original English text of EP 099 this looks as follows:
(1.1) Method for performing an electronic transaction between a first transaction party and a second transaction party
(1.2) using an electronic device operated by the first transaction party,
(1.3) the electronic device having an operating system creating a run-time environment for user applications,
(1.4) the method comprising: providing authentication data in a memory of said electronic device,
(1.5) said memory being a secure part of a Basic In Out System or any other secure location in said electronic device,
(1.6) which authentication data are inaccessible to a user of said electronic device,

[7] G 2/10 of 30 August 2011, ECLI:EP:BA:2011:G000210.20110830.
[8] Compare Court of The Hague 25 September 2019, ECLI:NL:RBDHA:2019:10064, paragraph 4.28.

(1.7) wherein the authentication data are encrypted when the authentication data are stored in said memory,
(1.8) a decryption key for decrypting the authentication data being incorporated in the electronic device,
(1.9) said decryption key being inaccessible to said user, to any user-operated software and to said operating system,
(1.10) wherein said memory is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user;
(1.11) providing authentication software in said electronic device,
(1.12) the authentication data being accessible to said authentication software, wherein authentication software is stored in said secure memory inaccessible to said operating system;
(1.13) activating the authentication software to generate a digital signature from the authentication data,
(1.14) wherein the authentication software is run in a secure processing environment inaccessible to said operating system;
(1.15) providing the digital signature to the second transaction party.

5.14. Samsung c.s. states - inter alia - that features 1.5 and 1.12 contain added matter. Feature 1.5 was not included at all in claim 1 of the original application and the measure ‘wherein authentication software is stored in said secure memory inaccessible to said operating system' did not form part of feature 1. 12 (see 2.17).

5.15. Samsung c.s. argues, with reference to various passages in the description of the originally filed application, that the said added features contain matter which is not covered by the originally filed application, in so far as those features include that:
i. the *authentication data* is securely stored in a memory of the electronic device; according to Samsung c.s. this secure storage is only disclosed in WO 752 in so far an authentication table is concerned;
ii. the memory of the electronic device in which the authentication data and the authentication software are stored may also be a part of the electronic device other than a location in the BIOS or a location accessible only by the BIOS; according to Samsung c.s. WO 752 only discloses, as they call it, 'BIOS-embodiments’.

5.16 DTS contests Samsung c.s.’ arguments. According to DTS, several extracts from the description of WO 752 provide a separate and interrelated basis for the additions in sub-features 1.5 and 1.12 above.

5.17 The District Court will first discuss part ii. of the argument of Samsung c.s. set out under 5.15 and, in its assessment thereof, will assume that where the originally submitted application refers to an authentication *table*, the person skilled in the art will also read authentication *data.*

5.18. First and foremost, the District Court states that the description of WO 752 starts (page 2, l. 7 up to and including page 6, l. 13) with a general description of all the intended embodiments of that application.

Next, embodiments in which the storage locations of the authentication data and the authentication software are not accessible to the operating system are described as the first embodiment (page 6, r. 14 through page 10, l. 35) and as the second embodiment (page 10, l. 36 through page 15, l. 10). Figures 1, 2 and 3 belong to these two embodiments. The third embodiment described later (page 15, l. 11 to page 29), which includes Figures 4 to 10, discloses that the operating system does have access to these storage locations. Data and software are only protected by encryption. This third embodiment is not protected by the claims of the patent as granted. After all, all claims require (feature 1.10) that the storage location for authentication data and software is secure because the operating system does not have access to it. In the following, the District Court therefore takes as a starting point that the third embodiment in the description of WO 752 and the accompanying figures, is not an embodiment of the invention for which a patent has been granted in EP 099.

5.19. According to DTS there is basis for feature 1.5 in the following passage of WO 752 (on page 6, l. 8-13, emphasis added by the court): "However, as is described hereinafter, the method according to the present invention *may employ* such a BIOS system to securely store certain digital data and/or such a BIOS system may be provided with an encryption system. A secure storage location and/or an encryption system are *not essential* to the BIOS system with respect to the present invention." From this, DTS understands that the authentication data does not necessarily need to be stored in a location that is part of the BIOS, but that it can be any storage location.

5.20. With Samsung c.s., the District Court is of the opinion that the average person skilled in the art will not understand from this passage what DTS argues. If the person skilled in the art reads the entire paragraph from which this passage originates (page 5, l. 31 up to and including page 6, l. 14, see 2.16), he will understand from this that the invention requires equipment that has a Basic Input/Output System such as a 'BIOS' or 'Boot agent' (where the court hereinafter refers to a BIOS, this also refers to other start-up systems comparable to those for the person skilled in the art on the priority date). This is evident from the following passages, among others:
- "(...) a new device relates to any electronic device containing a Basic In Out System ("BIOS", "Boot agent", etc.) with any associated secure storage/memory location" (page 5, l. 34-36); and
- "(...) an existing device relates to any electronic device containing a Basic In Out System" (pagina 6, l. 3 en 4).
In the passage "a secure storage location (...) is not essential to the BIOS system with respect to the present invention" the average person skilled in the art will read no more than that the *secure location* in the device in which the authentication table or data is stored can also lie outside the BIOS. The average person skilled in the art will not unambiguously read that it is not required that the electronic device is equipped with a BIOS, nor that every storage location in the equipment is a secure storage location.

5.21. In addition, the passage invoked by DTS is taken from the general part of the description of WO 752. This part is followed by the description of the three embodiments, as described in 5.18. Where this passage states that the invention can 'use' a BIOS to store digital data ('may employ'), the average person skilled in the art will understand this in such a way that it looks ahead to the

description of the third embodiment. It describes storage locations to which the operating system does have access. In this context, the Court refers to the passage on page 15, l. 11 through 14, which, in so far as relevant here, reads as follows: “In a third preferred installation method (...) the authentication data, (...) is stored in a memory that is accessible to an operating system of the device (...)”. However, as considered above under 5.18, it is precisely this embodiment that does not fall within the scope of protection of the claims as granted.

5.22. As basis for feature 1.5 DTS refers to more passages in the description of WO 752 relating to the third embodiment and figures belonging to that embodiment. This concerns in particular figures 5A and 5B, in which a storage location for the authentication data and software is disclosed that is not located in the BIOS. However, the third embodiment is an embodiment in which the authentication data and authentication software are stored in a memory accessible by the operating system of the electronic device (see page 15, l. 11 to 14, and page 18, l. 29 to 31). As considered above, that embodiment is not covered by the claims as granted. Indeed, the core of the granted claims is, as argued by DTS itself, that the memory in which the authentication data and authentication software are stored is not accessible to the operating system (and therefore to the user). In this respect, the Court refers to the following passage from the writ of summons: *'The essence of the patent is (...) that data is stored and processed in a secure area that is not accessible to the operating system and the user of the mobile device and to which unauthorized third parties cannot gain access”*[9] In the passages referred to by DTS in this context, it is also not mentioned that the features of the third embodiment can also be applied in the first embodiment (installation of the invention in a new electronic device) and the second embodiment (installation of the invention in an existing electronic device). This cannot be deduced from the above figures either.

5.23. DTS, referring to a decision of the TBA of the EPO, registered under number T 0667/08[10], argued that even if a particular embodiment does not fall within the scope of protection of the claims granted, the patent proprietor may nevertheless refer to the description and drawings accompanying that embodiment in order to substantiate his claim that the subject matter of the claims granted is covered by the originally filed application.
It can be deduced from the aforementioned decision that the person skilled in the art reads the application as a whole and can combine information from embodiments if the application as a whole and in particular the introductory description supports this. However, it cannot be deduced from this that structurally related measures from an embodiment (the storage location is not accessible for the operating system because this location is in the BIOS or is only accessible via the BIOS) can be expanded by adding an optional feature ("may employ a BIOS"), originating from an embodiment in which that measure is not related to the other structural features (in that embodiment the storage location is accessible for the operating system).

[9] Par. 20, fourth sentence
[10] Decision of 20 April 2012, ECL LEP:BA:20 12:1066708.20120420

5.24. More generally, DTS has also argued that the embodiments referred to in WO 752 are only examples and, as the District Court understands it, that the application in its entirety provides a basis for feature 1.5.

5.25. With DTS, the District Court is of the opinion that the average person skilled in the art will deduce from WO 752 that the location where the authentication data is stored does not necessarily have to be in the memory of the BIOS, but may be outside of it. However, the skilled person reading WO 752 in its entirety will learn from this that the inaccessibility for the operating system is created by the safe storage locations of the operating system being shielded by the BIOS. He learns this particularly from figure 3 of the second embodiment, in which a safe storage location outside the BIOS is disclosed, which can only exchange data with the BIOS and/or the authentication software stored in the BIOS. The description of WO 752 mentions this (on page 14):
- "In or behind the console 52, there is a secure area 62 only accessible to the BIOS. The secure area 62 comprises applications and storage locations, which are not reported to the operating system 48" (l. 12-15);
- "An authentication table may be securely stored in the secure storage location 60. In such a part of the computer, commonly seen as a part of the BIOS 44, the authentication table is unreachable for the operating system 48 and thus for the user" (l. 23-26); and
- "Therefore, the authentication software 54 may be installed in an application environment in the secure area 62 such that it may obtain the authentication table without passing through an unsecured part of the device" (l. 31-34).

5.26. The average person skilled in the art would also note from the originally filed application that if the authentication data is stored in a location outside the BIOS, not only the BIOS can access (and give instructions to) that authentication data, but also the authentication software can perform that function. After all, on page 10, l. 22 through 28 of the description of WO 752 of the first embodiment, the following is stated (italics included by the District Court):
"The encoded authentication table (for which the Court proposes to read: authentication data) is stored in a secure part of the BIOS, where it may only be retrieved by the BIOS and not by the operating system. This secure part of the BIOS may also be any other secure location in the device. For instance, it may be a separate part of a hard drive of a computer, which part may not be *accessible* to the operating system, but *only to the BIOS and/or authentication software."* Further, this passage should be read in conjunction with the rest of the description of the same embodiment: "The fifth column of Fig. 1 represents the actions of the authentication software, which (...) is stored in the BIOS" (p. 7, l. 23 to 25) and "According to cell 4, a BIOS manufacturer embeds or installs authentication software in the BIOS" (p. 8, l. 24-25). With regard to the authentication software it is further mentioned that it "runs in a separate operating environment in the BIOS or in a console and is independent from and inaccessible to the operating system (OS) on the device" (p. 7, l. 31-34).

5.27. The person skilled in the art therefore learns from all this that only the BIOS or the authentication software stored in the BIOS has access to the authentication data, so that the secure storage location is only created by the BIOS shielding it. This is perhaps most evident from the above cited passage: "Therefore, the authentication software 54 may be installed in an application environment in the secure area

62 such that it may obtain the authentication table without passing through an unsecured part of the device" (p. 14, l. 31-34).

5.28. In support of its claim that a BIOS does not play an essential role in the invention, DTS has further referred to the wording of the originally submitted claims, more specifically to those of claim 1 and (dependent) claim 13; claim 1 did not claim a BIOS. A BIOS is only mentioned for the first time in WO 752 in claim 13. Claim 1 of WO 752, however, does not contain as a feature 'a secure memory location' for authentication data or software either. The fact that a BIOS is not included in the main claim of WO 752 therefore does not say much about its function for a secure memory location, which was not included either.

5.29. DTS has further argued that support for its position can be found in the decision of the TBA of the EPO regarding the EP 140 application. This argument cannot be followed. At the time of the TBA decision the general part of claim 1 read as follows (see 2.5, italics included by the Court): `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 a Basic In Out System* and an operating system creating a runtime environment for user applications, *the electronic device having a memory comprising storage locations, part of the memory being accessible to the memory of the operating system, part of the memory being a secure area of the Basic In Out System, storage locations of which are not reported to the operating system by the Basic In Out System,* the method comprising: (...)'. It is true that the TBA considered the claims to be valid and did not consider the claims to contain added matter after the changes made by Ward, but it arrived at that conclusion because the claims explicitly included the role of the BIOS in the shielding of the authentication data and the authentication software of the operating system. This was different when the patent application was still pending before the examining division of the EPO. Ward then submitted an amendment to the claims, for which the Examination Division considered the following (par. 7.4 of the OD decision to reject the claims, see 2.4):
`Furthermore the description discloses the authentication data and software being unreachable and unknown to the operating system only in connection with the BIOS providing the function of controlling these. No other possible entity is disclosed. The features are therefore inextricably linked to the BIOS performing these functions instead and cannot be taken out independently.'

5.30. In this context, the District Court also refers to the opinion of the TBA with respect to the question whether the application of EP 140, as submitted to the TBA at the time, could be regarded as inventive. The TBA considered (see 2.5):
`The Board thus concludes that the subject-matter of claim 1 shows an inventive step over D12 [the closest prior art] alone (...), by virtue of the feature that the BIOS "shields" the secure area from the operating system.' The prosecution history of EP 140 therefore supports Samsung c.s.' position

5.31. In the foregoing, the District Court also took into account the fact that WO 752 does not describe any alternative for shutting off the access of the operating system/user of the electronic device to storage locations other than by means of the

BIOS. DTS also did not explain how the authentication data will be safely stored according to the patent if the BIOS is not granted a role in it.

5.32. All of the foregoing makes it clear that the average person skilled in the art will directly and unambiguously deduce from the original application that the security of transactions is achieved by storing the authentication data in a storage location within the BIOS or shielded from the operating system by the BIOS. However, this restriction resulting from the original application is not claimed in feature 1.5. The embodiments with an inextricable link to the BIOS are thus generalised to a more generic embodiment without that link. Thus, in the independent claim 1 that has been granted (i.e. insofar as it expresses that the authentication data can also be stored in 'any other secure location' in the electronic device), impermissible matter has been added.

5.33. DTS has also referred, as a basis for feature 1.12, to the dependent claim 26 of WO 752, which states as an additional/dependent feature that 'the authentication software is stored in a secure memory location inaccessible to the operating system'. DTS argues that claim 26 of WO 752 has simply been added to claim 1 as feature 1.12, so that WO 752 already clearly and unambiguously discloses that the authentication software can be stored in 'any secure location'. From what has been considered above with regard to feature 1.5, it follows that this defence must also be rejected. The average person skilled in the art reading WO 752 will interpret 'a secure memory location inaccessible to an operating system' in such a way that not only the authentication software itself is inaccessible to the operating system, but also its storage location is inaccessible to the operating system. He understands from the description that this is the case because the storage location of the authentication software is in or behind the BIOS. Therefore, feature 1.12 also contains added matter.

5.34. The independent system claim 23 contains the above listed features as well, so that the above conclusion also applies to that claim. Independent product claim 24 contains the same feature 5 (and an almost identical feature 12), so that the foregoing also applies to that claim.

5.35. This leads to the conclusion that Claims 1, 23 and 24 as granted should be invalidated. Claims 2 to 22 are all dependent on claim 1 and claim 25 is dependent on claim 24. Since Claims 1 and 24 are invalid for added matter, the dependent claims are invalid on the same grounds. Samsung c.s.'s counterclaim for the revocation of the Dutch part of EP 099 should therefore be granted.

5.36. DTS cannot, in view of the judgment in the counterclaim action, successfully argue infringement of the Dutch part of EP 099 by Samsung c.s. in the main action. To that extent, the claims of DTS are ready to be rejected. To the extent DTS's claims are based on Samsung c.s.'s infringement of the foreign parts of EP 099 (see 2.3), Samsung c.s.'s defense that there is no infringement of a valid patent has the same basis. In view of the provisions of Article 24(4) Brussels I bis Regulation, the Court has no jurisdiction to rule on Samsung c.s.'s invalidity defenses for the foreign parts of EP 099. At the hearing, DTS requested that the proceedings be suspended

insofar as the infringement of the foreign parts of EP 099 is concerned until it is established whether those parts are valid or not. The Court shall grant that request.[11] In view of the judgment on the Dutch part of EP 099 and the ongoing opposition proceedings against EP 099, the Court sees no reason to assess whether Samsung c.s.'s products would infringe a foreign part of EP 099 (as currently drafted), nor to address Samsung c.s.'s other defenses against the claims.

*EP 140*

5.37. The District Court adopts the division into features by the parties of the independent method claim 1 of EP 140. This division looks as follows in the original English text of EP 140:
(1.1) Method for performing an electronic transaction between a first transaction party and a second transaction party,
(1.2) using an electronic device operated by the first transaction party,
(1.3) the electronic device having an operating system creating a run-time environment for user applications,
(1.4) and authentication software running in a separate operating environment, independent from and inaccessible to said operating system,
(1.5) 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 storage locations of which are not reported to the operating system,
(1.6) the method comprising: providing authentication data in the secure area of said electronic device, which authentication data are inaccessible to a user of said electronic device, wherein said secure area is inaccessible to said operating system of said electronic device, thereby rendering the authentication data inaccessible to said user,
(1.7) providing authentication software in said electronic device, the authentication data being accessible to said authentication software,
(1.8) wherein the authentication software is stored in the secure area inaccessible to said operating system,
(1.9) activating the authentication software to generate a digital signature from the authentication data,
(1.10) wherein the authentication software is run in a secure processing environment inaccessible to said operating system,
(1.11) providing the digital signature to the second transaction party.

5.38. The Independent System Claim (Claim 23) and the Independent Product Claim (Claim 24) also contain the features listed above.

5.39. Samsung c.s. states - inter alia - that the features 1.5, 1.6, and 1.8 contain added matter. Features 1.5 and 1.8 were not included in Claim 1 of the original application. The parts of feature 1.6 shown in italics below did not form part of claim 1 of the original application: ‘the method comprising: providing authentication data in *the secure area of* said electronic device, *which authentication data are inaccessible to a user of said electronic device, wherein said secure area is inaccessible to said*

[11] HR 30 November 2007, ECLI:NL:HR:2007:BA9608 (Roche-Primus II)

*operating system of said electronic device, thereby rendering the authentication data inaccessible to said user'* (see 2.17).

5.40. Samsung c.s. argue with reasons and reference to various passages from the description of WO 752 that these features contain inadmissible added matter, because the application does not express that:
i. the - single - memory of the electronic device contains a combination of parts that are accessible and not accessible to the operating system; according to Samsung c.s., WO 752 only discloses an embodiment with two physically separate memories, one accessible to the operating system and the other not (shown in Figure 3) and an embodiment with a memory accessible to the operating system (shown in Figure 5A), and these embodiments cannot be combined with each other;
ii. the *authentication data* is securely stored in an electronic device memory; according to Samsung c.s., this secure storage is only disclosed as far as an authentication table is concerned;
iii. other than by storage in or behind the BIOS, it is realised that (parts of) the memory where the authentication data and the authentication software is stored does not report to the operating system; according to Samsung c.s. the absence of reporting to the operating system is only disclosed in figure 3 of WO 752 and this concerns, as they call it, a `BIOS embodiment'.

5.41. DTS contests the argument of Samsung c.s. According to DTS various paragraphs from the description of WO 752, separately and in conjunction with each other, provide basis for the additions in features 1.5, 1.6 and 1.8.

5.42. In the following, the District Court assumes conclusively that basis can be found in the originally filed application for the presence in the electronic device of a memory which is divided into two parts and that, where the originally filed application refers to an authentication table, authentication data may also be read. The court also leaves in the middle whether only Figure 3 may be regarded for that argument, or also Figure 5A.

5.43. In the opinion of the District Court, the average person skilled in the art will read the feature concerning the `not reporting' of the memory location in which the authentication data is stored to the operating system (and thus the user) in such a way that this - among other things - means that the operating system does not have access to that location.

5.44. The question that then remains is the same as the one on which the District Court ruled with regard to the features 1.5 and 1.12 of claim 1 of EP 099 and the corresponding features of the independent claims 23 and 24 of that patent, namely the question what the originally filed application discloses about the way in which the location in the electronic device where the authentication data and authentication software are stored, is shielded from the operating system of the electronic device and thus from the user of that device, so that it qualifies as safe (`secure').

5.45. The District Court considered, in relation to EP 099, that it is of the opinion that the average person skilled in the art will deduce from the originally filed application that

it is exclusively the BIOS of the electronic device that performs the function of 'shield' between the operating system (and the user) of the electronic device on the one hand and the memory locations in the device where authentication data and authentication software are stored on the other. Because of that function of the BIOS, the operating system (and the user) are unable to access that data and software and are therefore unaware of it, and to that extent the BIOS is essential for the invention embodied in EP 099. This then led the court to conclude that the independent claims of EP 099 are invalid because the matter of the claims contains matter that was not clearly and unambiguously disclosed in WO 752.

5.46. The arguments put forward by DTS against the added matter objection of Samsung c.s. concerning EP 140 are the same as it raised in response to Samsung c.s.'s added matter objection concerning EP 099. These arguments have already been discussed and rejected in the context of the assessment of the validity of EP 099.

5.47. With regard to the independent claims of EP 140, the conclusion must therefore be that these also contain added matter as they not do justice to the necessary presence and function of the BIOS of the electronic device resulting from the application originally filed. These independent claims are therefore invalid.

5.48. As with EP 099, all other claims (2 – 22 and 25) of EP 140 are dependent on one of the independent claims. They are therefore invalid for the same reasons. Samsung c.s.'s counterclaim for revocation of the Dutch part of EP 140 should therefore be granted.

5.49. DTS cannot, in view of the judgment in the counterclaim proceedings, successfully argue infringement by Samsung c.s. on the Dutch part of EP 140. To that extent, the claims of DTS are ready to be dismissed. To the extent DTS's claims are based on Samsung c.s.'s infringement of the foreign parts of EP 140 (see 2.3), Samsung c.s.'s defense that there is no infringement of a valid patent has the same basis. In view of the provisions of Article 24(4) Brussels I bis Regulation, the Court has no jurisdiction to adjudicate Samsung c.s.'s nullity defences in respect of the foreign parts of EP 140. At the hearing, DTS requested that the proceedings in the main action with respect to the infringement of the foreign parts of EP 140 would be suspended until it is established whether those parts are valid or not. The court upheld that request. In view of the judgment on the Dutch part of EP 140 and the ongoing opposition proceedings against EP 140, the court sees no reason to assess whether Samsung c.s.'s products would infringe a foreign part of EP 140 (as currently drafted), nor to comment on Samsung c.s.'s other defences against the claims.

*Conclusion*

5.50. As for the assessment of the alleged patent infringement of foreign parts of EP 099 and EP 140 the judgement on the validity of those parts of the competent judges of the designated countries listed in 2.3 must be awaited, the court will stay any further decision in both cases.

Either party may bring one or both of the cases on the docket as soon as one or more final decisions of competent foreign courts are known on the nullity objections of Samsung c.s. against EP 099 and/or EP 140, or as soon as it is established that DTS no longer defends the patents in the designed countries or Samsung c.s. no longer contests their validity.

## 6. The decisions

The court

In Case I:

*in the main action and the counterclaim proceedings*

6.1. Stays any further decision;

6.2. provides that the either party can place the case on the docket at the moment described in more detail in the last sentence of par. 5.50;

In Case II:

*in the main action and the counterclaim proceedings*

6.3. Stays any further decision;

6.4. provides that the either party can place the case on the docket at the moment described in par. 5.50, last sentence.

This judgment was rendered by F.M. Bus, J.E. Bierling and H. Meinders and pronounced in public by D. Nobel, judge, on May 13, 2020.