

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

THE HILLMAN GROUP, INC.,

Petitioner,

v.

HY-KO PRODUCTS COMPANY LLC,

Patent Owner.

Case No. IPR2023-00076
U.S. Patent No. 11,227,455

PETITION FOR *INTER PARTES* REVIEW

Table of Contents

I.	PRELIMINARY STATEMENT	1
II.	PRECISE RELIEF REQUESTED	2
	A. Claims for Which Review Is Requested	2
	B. Statutory Grounds.....	2
III.	THE '455 PATENT	3
IV.	LEVEL OF SKILL IN THE ART	6
V.	CLAIM CONSTRUCTION	6
VI.	CLAIMS 1-6 OF THE '455 PATENT ARE UNPATENTABLE	7
	A. Prior Art.....	7
	1. Chies.....	7
	2. Marsh.....	9
	B. Grounds 1 and 2: Chies Anticipates and/or Renders Obvious Claims 1 and 3.....	12
	1. Independent Claim 1	12
	1(pre): A method for duplicating an access device, comprising:	12
	1(a): providing a first computing device configured to communicate with a transmitter/receiver device (t/r device), the t/r device including an antenna for wirelessly communicating with a master key for a vehicle;.....	12
	1(b): running a cloning application associated with said t/r device on the first computing device, the cloning application configured to electronically communicate with the t/r device;	15

1(c): retrieving, by the antenna of the t/r device, security information digitally stored by said master key;	15
1(d): communicating, by the cloning application, the security information for said master key to said network server;	18
1(e): generating, by the network server, a cloning security information;.....	19
1(f): communicating, by the network server, the cloning security information to the cloning application; and.....	20
1(g): transmitting, by the cloning application, the cloning security information to the t/r device to program an electronic access device of a generally programmable duplicate key with the cloning security information.....	25
2. Claim 3: The method of claim 1, further comprising: in response to communicating, by the cloning application, the security information for said master key to said network server, determining, by the network server, whether the security information is encrypted; and generating the cloning security information.	28
C. Ground 3: Chies and Marsh Render Claims 2-6 Obvious.	30
1. Claim 2:.....	30
2(pre): “The method of claim 1, further comprising:”	30
2(a): “in response to retrieving, by the t/r device, security information from said master key,”	31
2(b): “determining, by the cloning application, whether the security information is encrypted and”	31
2(c): “generating the cloning security information”	36
2. Claim 3: The method of claim 1, further comprising: in response to communicating, by the cloning application,	

	the security information for said master key to said network server, determining, by the network server, whether the security information is encrypted; and generating the cloning security information.	40
3.	Claim 4:	43
	4(pre): The method of claim 1, further comprising:	43
	4(a): capturing at least one image of a blade of said master key,	43
	4(b): communicating said at least one image of said blade to said network server,	46
	4(c): cutting a duplicate blade of a generally programmable duplicate key, and	48
	4(d): providing said generally programmable duplicate key to said customer.	49
4.	Claim 5: The method of claim 1, further comprising: placing said generally programmable duplicate key in proximity with said vehicle, sampling communications between said generically programmable duplicate key and said vehicle to generate authentication sample data.	51
5.	Independent Claim 6	54
	6(pre): A vehicle access device duplication system comprising:	54
	6(a): a non-transitory computer-readable storage medium storing executing instructions that, when executed, cause a cloning application to perform steps comprising:	54
	6(b): determining that a first device of a customer is communicating with a transmitter/receiver device (t/r device), the t/r device including an antenna ring for wirelessly communicating with an access device for a vehicle;	57

6(c): retrieving security information digitally stored by said access device;	63
6(d): communicating the security information for said access device to a network server;.....	65
6(e): generating a cloning security information; and.....	67
6(f): transmitting the cloning security information to the t/r device to program a duplicate access device with the cloning security information; and.....	67
6(g): a processor configured to execute the instructions.	68
VII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION TO DENY INSTITUTION	70
A. The Board Should Not Deny Institution Under § 325(d).....	70
B. The Board Should Not Deny Institution Under § 314(a).....	71
VIII. GROUNDS FOR STANDING.....	72
IX. MANDATORY NOTICES	72
A. Real Party-in-Interest	72
B. Related Matters.....	72
C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)	72
D. Service Information Under 37 C.F.R. § 42.8(b)(4).....	73
X. CONCLUSION.....	73

LIST OF EXHIBITS

Exhibit	Description
Ex. 1001	U.S. Patent No. 11,227,455 to Mutch et al.
Ex. 1002	Declaration of Paul Clark
Ex. 1003	Prosecution History of U.S. Pat. No. 11,227,455
Ex. 1004	WO 2008/145199A1 to Chies et al. (“Chies”)
Ex. 1005	U.S. Patent No. 9,563,885 to Marsh et al. (“Marsh”)
Ex. 1006	U.S. Patent No. 10,013,833 to Blalock et al. (“Blalock”)
Ex. 1007	U.S. Pat. App. Pub. No. 2015/0050094 to Gerlings (“Gerlings”)

I. PRELIMINARY STATEMENT

Petitioner The Hillman Group, Inc. requests *inter partes* review of claims 1-6 of U.S. Patent No. 11,227,455 (Ex. 1001), assigned to Hy-Ko Products Company LLC.

The '455 patent relates to “a distributed cloning system, and method for replacement, generation, or reprogramming of vehicle access devices, such as transponder keys or remotes.” Ex. 1001, 1:18:21. The key duplication system uses a “transmitter/receiver device (‘t/r device’)” that can receive information from a vehicle key. Ex. 1001, 2:25-45. The t/r device may transmit the key information to a network server to generate “cloning security information” that the t/r device then transmits to a “duplicate access device” (i.e., blank transponder key) to program a duplicate key. *Id.*

During prosecution, the Examiner failed to consider prior art disclosing several elements of claims 1 and 6, including the claimed “t/r device including an antenna ring for wirelessly communicating with an access device for a vehicle” and “retrieving security information digitally stored by said access device.” Ex. 1003, 157 (emphasis in original).

The Examiner failed to consider the prior art presented in this Petition, which anticipates and/or would have rendered obvious claims 1-6. Accordingly,

Petitioner requests that the Board institute *inter partes* review and cancel the claims.

II. PRECISE RELIEF REQUESTED

A. Claims for Which Review Is Requested

Petitioner respectfully requests *inter partes* review under 35 U.S.C. § 311 of claims 1-6 of the '455 patent and cancellation of those claims.

B. Statutory Grounds

Each asserted reference identified in the table below was filed before (and issued before) March 18, 2018, the earliest possible priority date of the '455 patent, and is prior art under 35 U.S.C. § 102(a).

Prior Art References
WO 2008/145199A1 to Chies et al. ("Chies," Ex. 1004), published December 4, 2008.
U.S. Patent No. 9,563,885 to Marsh et al. ("Marsh," Ex. 1005), filed July 6, 2015, and issued February 7, 2017.

Claims 1-6 of the '455 patent are unpatentable under 35 U.S.C. §§ 102 and/or 103 based on the following grounds:

Grounds of Unpatentability	
1	Chies anticipates claims 1 and 3 under 35 U.S.C. § 102.
2	Chies renders obvious claims 1 and 3 under 35 U.S.C. § 103.
3	Chies in combination with Marsh renders obvious claims 2-6 under 35 U.S.C. § 103.

III. THE '455 PATENT

Independent claim 1 recites:

1. A method for duplicating an access device, comprising:
providing a **first computing device** configured to communicate with
a **transmitter/receiver device (t/r device)**, the **t/r device**
including an **antenna** for wirelessly communicating with a
master key for a vehicle;
running a cloning application associated with said **t/r device** on the
first computing device, the cloning application configured to
electronically communicate with the **t/r device**;
retrieving, by the **antenna** of the **t/r device**, security information
digitally stored by said **master key**;

communicating, by the cloning application, the security information
for said **master key** to said **network server**;
generating, by the **network server**, a cloning security information;
communicating, by the **network server**, the cloning security
information to the cloning application; and
transmitting, by the cloning application, the cloning security
information to the **t/r device** to program an electronic access
device of a **generally programmable duplicate key** with the
cloning security information.

Ex. 1001, 9:58-10:19; Ex. 1002 ¶30.

As shown in annotated Figure 4 below, the '455 patent discloses a first
computing device (computing device 100, **green**), a t/r device (t/r device 10, **blue**),
an antenna of the t/r device (antenna 40, **orange**), a master key for a vehicle
(master key 20, **purple**), a network server (network server 130, **red**), and a
generally¹ programmable duplicate key (generically programmed duplicate
electronic access device 22', **yellow**). Ex. 1001, 7:30-67; Ex. 1002 ¶31.

¹ The '455 patent alternatively refers to the duplicate key of element 50 as a
“generically programmable duplicate key,” “generically programmed duplicate

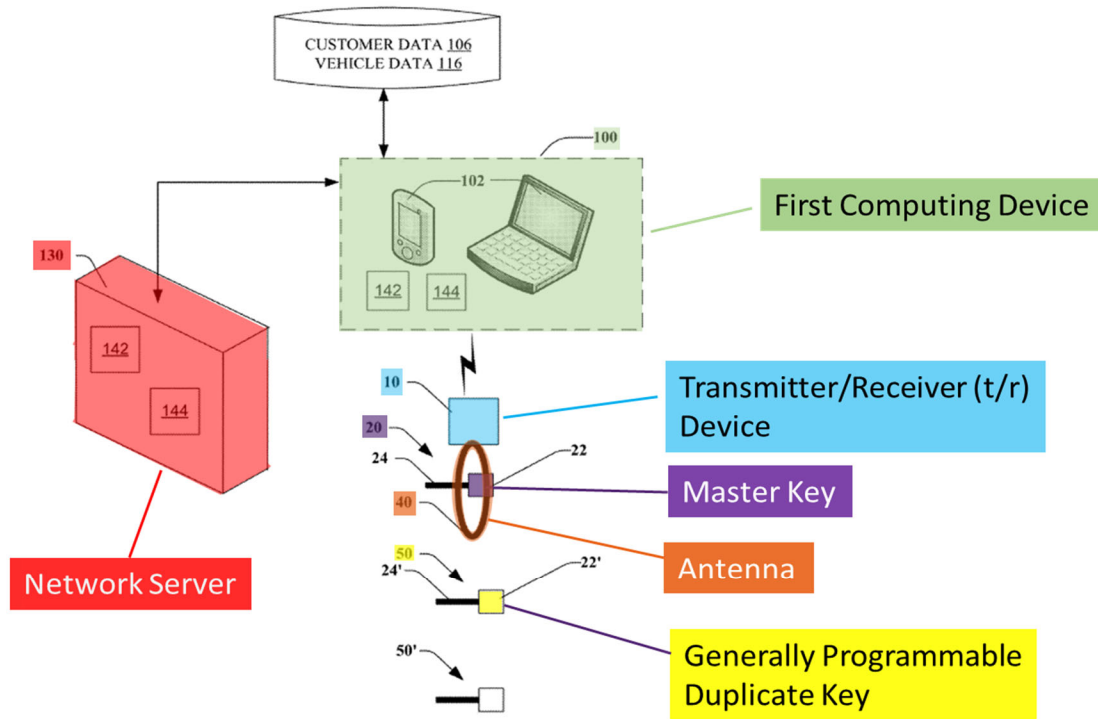


FIG. 4

The t/r device reads the security information on the master key and transmits the information to the network server via the cloning application of the computing device. Ex. 1001, 7:30-67. The network server then processes the security information from the master key, e.g. by decrypting the security information, and

key,” “generally programmed duplicate key,” and generally programmable duplicate key.” *See, e.g.*, Ex. 1001, 6:7-16, 6:61-67, claim 1. For purposes of this Petition only, Petitioner treats these terms as interchangeable and as generally designating a programmable blank transponder key. Ex. 1002 ¶31 n.1.

generates cloning security information that is transmitted to the generally programmable duplicate key via the antenna of the t/r device to create a duplicate of the master key. *Id.*, 7:14-67; Ex. 1002 ¶32.

IV. LEVEL OF SKILL IN THE ART

A person of ordinary skill in the art (“POSITA”) at the time of the alleged invention would have had a degree in engineering and three years of experience in key duplication equipment. Ex. 1002 ¶36. This level of skill is approximate, and more experience would compensate for less formal education, and vice versa. *Id.* For example, an individual having no degree in engineering but ten years of key duplication experience would qualify as a POSITA. *Id.* Moreover, a person with no key duplication experience but a masters or doctorate in engineering may also qualify as a POSITA. *Id.* Experience in the field of key duplication equipment may include experience with various types of key duplication equipment, including vending machines. *Id.* Additional education could substitute for professional experience and vice versa. *Id.*

V. CLAIM CONSTRUCTION

The Board construes claims in accordance with 37 C.F.R. § 42.100(b) and *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). Claims only need to be construed to the extent necessary to resolve a controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir.

2017). No claim terms of the '455 patent need construction because the claims encompass the prior-art mappings provided below under any construction consistent with *Phillips*.² Ex. 1002 ¶38.

VI. CLAIMS 1-6 OF THE '455 PATENT ARE UNPATENTABLE

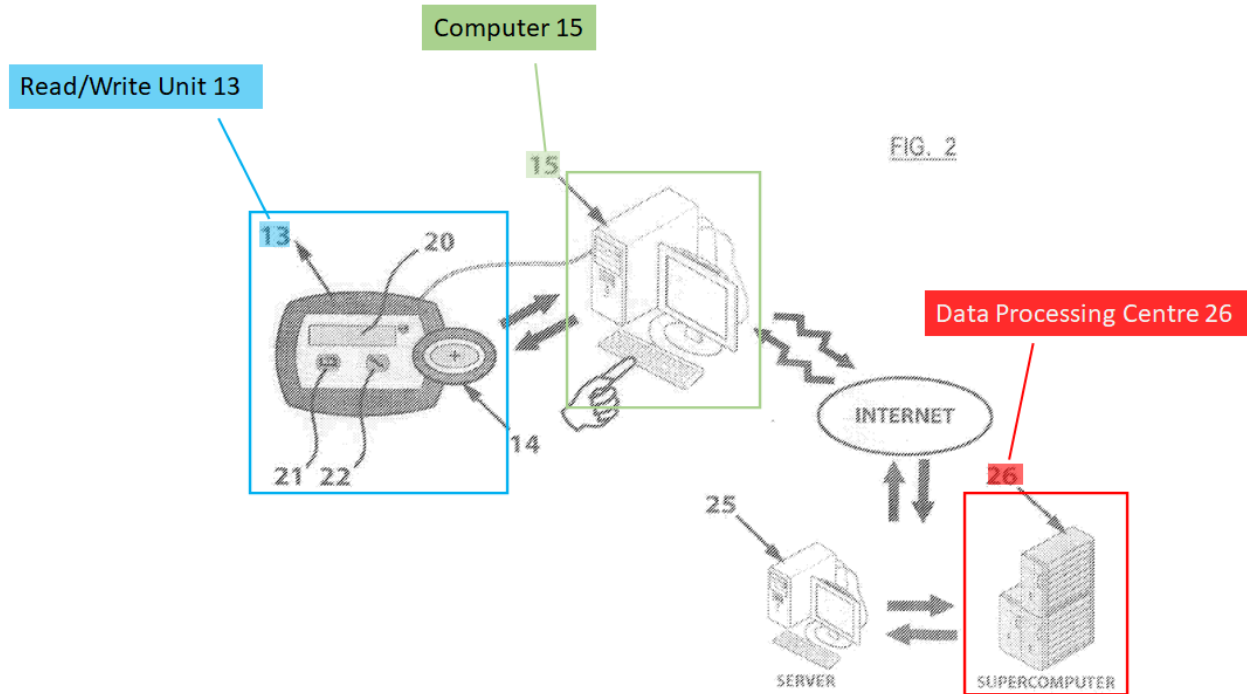
A. Prior Art

1. Chies

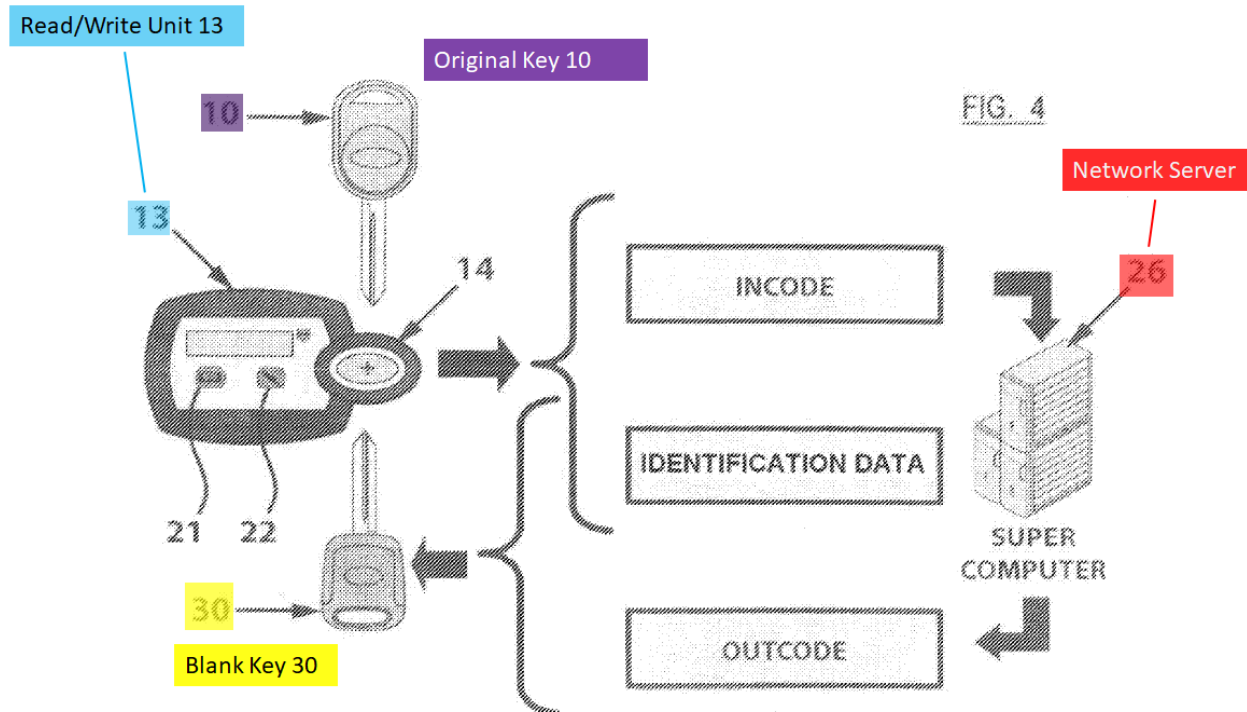
Chies discloses a method for duplicating “electronic-code keys” with “code-based electronic recognition means,” such as keys used in motor vehicle starting systems. Ex. 1004, 1:10-17. For example, Chies discloses duplicating key 10 by inserting it into a read/write unit 13 (blue in annotated Figure 2 below) and establishing wireless communication with the key via the antenna of the read/write unit 13. *Id.*, 4:26-5:2, Fig. 2. The read/write unit 13 is connected to a computer 15 (green below), which runs an “application program that is adapted to handle the flow of data coming in from the read/write unit 13.” *Id.*, 5:33-6:4. The computer 15 is connected to a network (e.g., the Internet) and transmits key information to

² Because the IPR procedure does not permit challenges under 35 U.S.C. § 112, Petitioner has not included any indefiniteness arguments herein but may present such arguments in other proceedings.

remote servers including server 25 and data processing centre 26 (**red** below). *Id.*, 5:33-6:28; Ex. 1002 ¶41.



After receiving the master key security information transmitted from read/write unit 13 in the form of “INCODE” data, data processing centre 26 processes the key information, such as by decrypting the INCODE data, to prepare “OUTCODE” data for programming a blank key. Ex. 1004, 6:30-8:9, 8:21-34. The data processing centre 26 sends the OUTCODE data to read/write unit 13, which writes the data to the microchip of blank key 30 (**yellow** in annotated Figure 4 below) to create a duplicate of original key 10 (**purple** below). *Id.*, 8:11-34, Fig. 4; Ex. 1002 ¶42.



Chies is within the same field of endeavor as the '455 patent, transponder key duplication, and is analogous prior art. *Donner Tech., LLC v. Pro Stage Gear, LLC*, 979 F.3d 1353, 1359 (Fed. Cir. 2020); Ex. 1002 ¶¶41-43.

2. Marsh

Marsh discloses systems and methods for duplicating transponder keys and managing associated key information. Ex. 1005, 1:1-16. For example, Marsh discloses a system including key duplication kiosk 200 (green in annotated Figs. 2 and 13 below), which includes a transponder antenna 1302 that reads information from a transponder chip 1306 of transponder key 1304 inserted into the kiosk (purple below). Ex. 1005, 1:54-3:14, 16:23-42, Figs. 2, 13. The kiosk may transmit the key information to server 1310 (red below) over a communication

network, and server 1310 then processes the information, e.g., to create a duplicate key. Ex. 1005, 17:51-18:9, 25:61-65; Ex. 1002 ¶44.

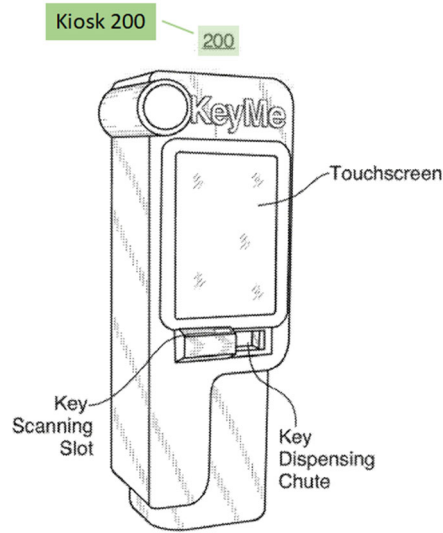


FIG. 2

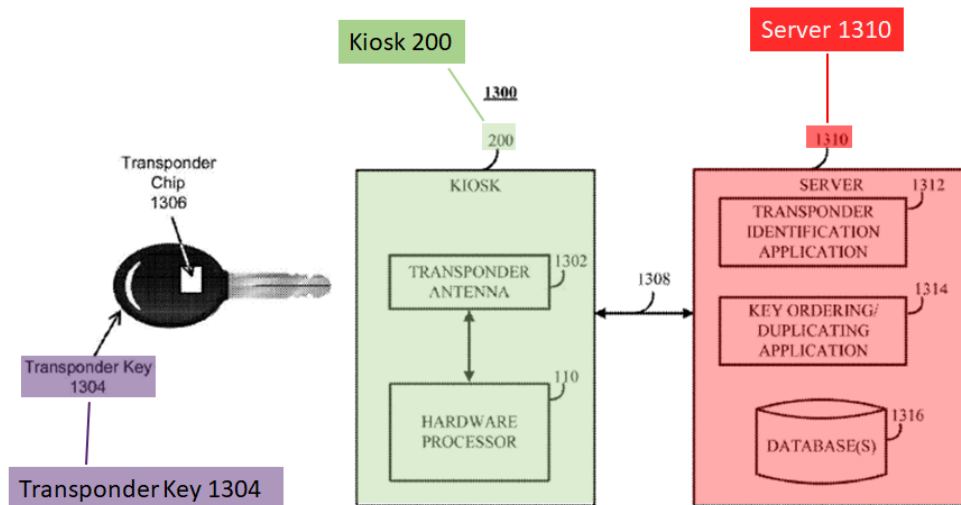
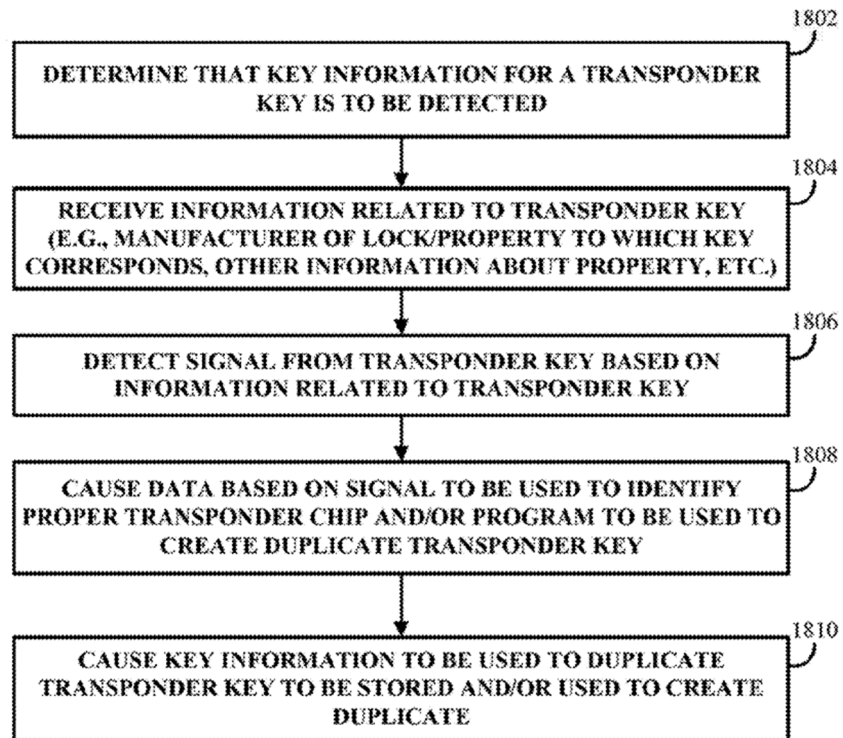


FIG. 13

Marsh also discloses a process of reading information from a transponder key to duplicate the key, as shown in the flow chart of Figure 18 below. Ex. 1005,

22:25-25:65, Fig. 18. The process includes detecting a signal from the transponder key, using that signal to identify a proper transponder chip for use in a key blank, and using the key information to duplicate the transponder key. *Id.*



Marsh is also within the same field of endeavor as the '455 patent, transponder key duplication, and is analogous prior art. *Donner*, 979 F.3d at 1359; Ex. 1002 ¶¶44-46.

B. Grounds 1 and 2: Chies Anticipates and/or Renders Obvious Claims 1 and 3.

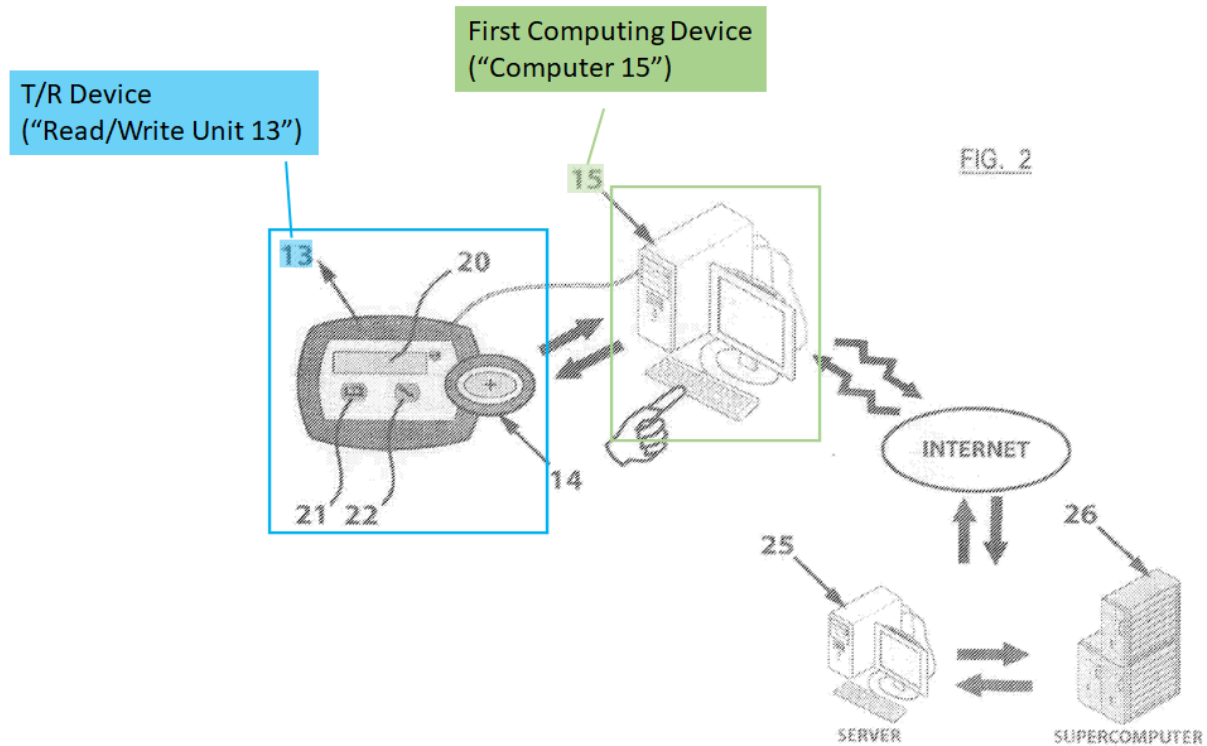
1. Independent Claim 1

1(pre): A method for duplicating an access device, comprising:

If the preamble is limiting, Chies discloses a method for duplicating an access device. The '455 patent describes “vehicle access devices” as including “transponder keys or remotes.” Ex. 1001, 1:18-21, 2:12-14. Chies similarly describes systems and methods for duplicating “keys provided with code-based electronic recognition means,” including transponder keys. Ex. 1004, 1:10-17, 4:26-29; Ex. 1002 ¶47.

1(a): providing a first computing device configured to communicate with a transmitter/receiver device (t/r device), the t/r device including an antenna for wirelessly communicating with a master key for a vehicle;

Chies discloses the use of a first computing device (e.g., computer 15) that is configured to communicate with a t/r device (e.g., read/write unit 13). Ex. 1004, 5:33-34 (“The peripheral read/write unit 13 is connected to a computer 15, e.g. via a serial interface RS232 or a Universal Serial Bus (USB).”), 6:2-4 (“Installed in the same computer 15 there is an application program that is adapted to handle the flow of data coming in from the read/write unit 13.”), Fig. 2; Ex. 1002 ¶48.



A POSITA would have understood that Chies' read/write unit 13 is a "t/r device" because it is described as both transmitting information to (i.e., writing) and receiving information from (i.e., reading) devices such as transponder keys. Ex. 1004, 4:31-5:2, 6:6-13 ("The read/write unit 13 performs data reading and writing operations and is capable of identifying the type of key"), 6:30-7:19, 8:11-34; Ex. 1002 ¶49.

Chies further discloses that the read/write unit 13 includes an antenna for wirelessly communicating with a master key for a vehicle (e.g., key 10). Ex. 1004, 4:31-5:2 ("The code-based electronic recognition means is energized via an electromagnetic coupling established through an antenna of a read/write unit 13

adapted to receive a key 10 or 30 in a pit or hole 14 (see Figure 4).”), 6:6-13 (“[T]he read/write unit 13 is provided with . . . an antenna (not shown) for receiving and transmitting data”), 7:4-5 (“[A] wireless communication is then established between the read/write unit 13 and the code-based electronic recognition means 11 of the key 10.”); Ex. 1002 ¶50.

Chies further discloses that the read/write unit 13 communicates wirelessly with “original key 10 to be duplicated,” and that Chies’ method is applicable to motor vehicle keys such as those used “in connection with motor-vehicle starting systems.” Ex. 1004, 1:10-17, 6:30-7:5, 8:21-34. A POSITA would have understood that Chies’ “original key 10 to be duplicated” is the claimed “master key” because that term refers to an original key that is duplicated. *See* Ex. 1001, 4:27-29 (“Such vehicles typically include an original key that is a suitable match for the vehicle, commonly referred to as the master key.”), 4:47-49, 6:7-16; Ex. 1002 ¶51.

Chies thus discloses providing a first computing device configured to communicate with a transmitter/receiver device (t/r device), the t/r device including an antenna for wirelessly communicating with a master key for a vehicle. Ex. 1002 ¶¶48-52.

1(b): running a cloning application associated with said t/r device on the first computing device, the cloning application configured to electronically communicate with the t/r device;

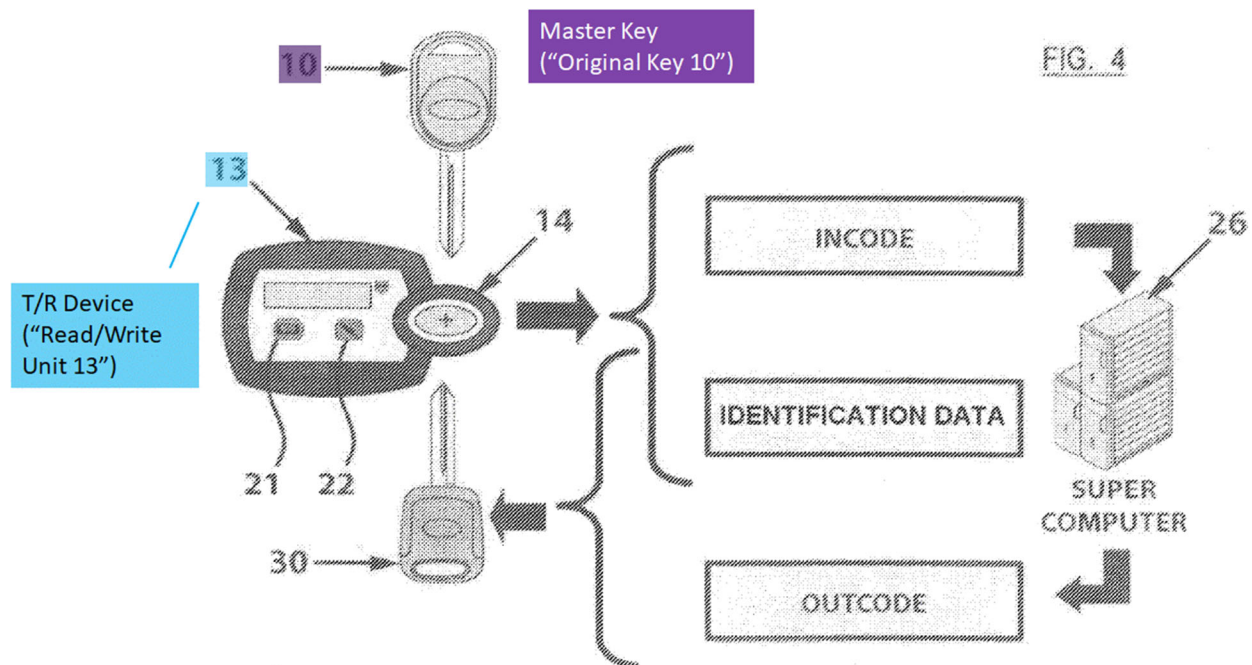
Chies discloses the use of a cloning application (e.g., the “application program”) that is associated with the t/r device (e.g., read/write unit 13) on the first computing device (e.g., computer 15), where the cloning application is configured to electronically communicate with the t/r device. Ex. 1004, 5:33-6:4 (“Installed in the same computer 15 there is an application program that is adapted to handle the flow of data coming in from the read/write unit 13.”), 7:12-19 (“The read/write unit 13 transmits the INCODE . . . to the computer connected thereto. The computer 15, as duly provided with the application program, receives such information and sends it to the serving computer or server 25.”); Ex. 1002 ¶¶53.

Chies thus discloses running a cloning application associated with said t/r device on the first computing device, the cloning application configured to electronically communicate with the t/r device. Ex. 1002 ¶¶53-54.

1(c): retrieving, by the antenna of the t/r device, security information digitally stored by said master key;

As discussed above for Claim 1(a), Chies discloses a t/r device (e.g., read/write unit 13) including an antenna for wirelessly communicating with a master key for a vehicle. Ex. 1004, 4:31-5:2, 6:6-13 (“[T]he read/write unit 13 is provided with . . . an antenna (not shown) for receiving and transmitting data”),

7:4-5 (“[W]ireless communication is then established between the read/write unit 13 and the code-based electronic recognition means 11 of the key 10.”). Chies further discloses retrieving security information digitally stored by the master key through those wireless communications. Ex. 1004, 5:4-14 (describing storing information digitally in memory on the key, including “identification data and a secret code of the key”), 6:30-7:19 (“[A] key 10 to be duplicated is introduced in the appropriate receptacle 14 of a read/write unit 13. Via the interactive read button 21, the read/write unit 13 reads the identification data of the key 10, thereby recognizing the type of key being handled, and temporarily stores such data in the internal memory thereof.”), Fig. 4; Ex. 1002 ¶¶48-52, 55.

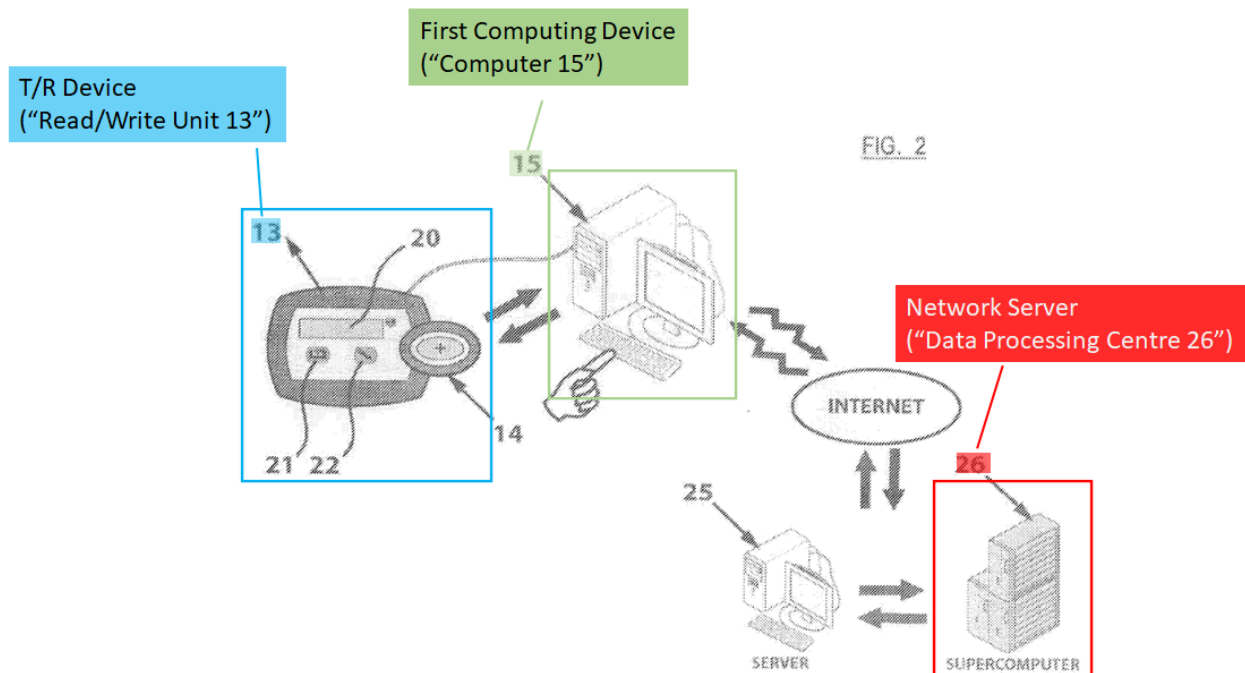


The information read from key 10 may be encrypted security information digitally stored on the key. Ex. 1004, 6:30-7:10 (“In the assumption that the key 10 is of the type with a secret (encrypted) code, the read/write unit 13 concurrently performs an inquiry operation to query the key 10. Such query occurs through a code that is implemented in the read/write unit 13 and is solely known by the manufacturer.”). Chies refers to the security information received from the master key by read/write unit 13 as “INCODE.” Ex. 1004, 7:8-10 (“What the read/write unit 13 acquires is therefore a data-based information that is encrypted at random in a first encryption form, which shall be defined as INCODE hereinafter.”), 7:29-8:9 (describing a process wherein “the INCODE is decrypted,” “the secret code is recognized and authenticated” such that “the single and sole secret code corresponding to the one contained in the microchip of the key 10 to be duplicated is acquired,” and “[t]he data processing centre 26 encrypts the corresponding secret code . . . into a second encryption form, which shall be defined as OUTCODE hereinafter.”); Ex. 1002 ¶56.

Chies thus discloses retrieving, by the antenna of the t/r device, security information digitally stored by said master key. Ex. 1002 ¶¶55-57.

1(d): communicating, by the cloning application, the security information for said master key to said network server;

Chies discloses a cloning application (e.g., the application program of computer 15) communicating the security information (e.g., the INCODE data) of a master key (e.g., key 10) to a network server (e.g., data processing centre 26). Ex. 1004, 6:15-7:31, Fig. 2; Ex. 1002 ¶58.



In particular, Chies discloses that read/write unit 13 transmits the INCODE data that it read from original key 10 to computer 15. Ex. 1004, 7:12-16. The “computer 15, as duly provided with the application program, receives such information and sends it to the serving computer or server 25.” *Id.*, 7:16-18. Server 25 then transmits the INCODE data to data processing centre 26 (to which server

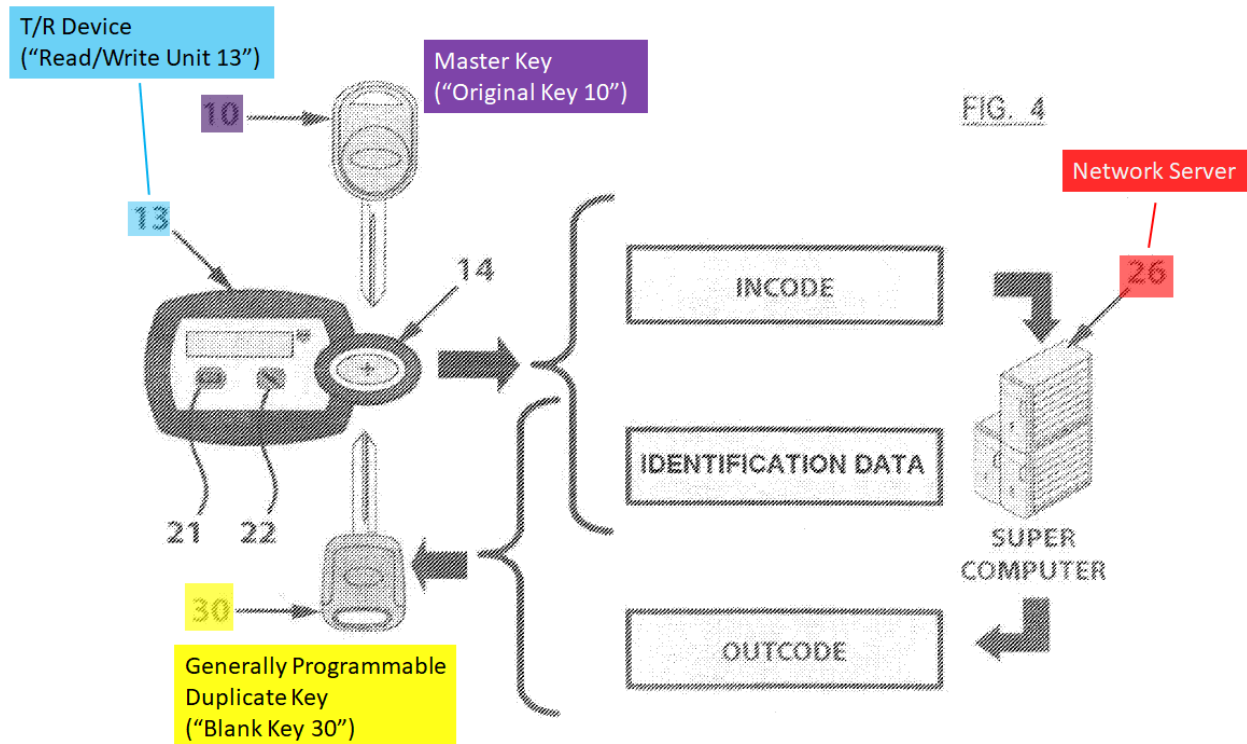
25 is connected over the Internet), where the INCODE data is processed. *Id.*, 6:15-28, 7:21-31.

Chies thus discloses communicating, by the cloning application, the security information for said master key to said network server. Ex. 1002 ¶¶58-60.

1(e): generating, by the network server, a cloning security information;

Chies discloses a network server (e.g., data processing centre 26) generating cloning security information (e.g., “OUTCODE” data). Ex. 1004, 7:29-8:9. The ’455 patent does not expressly define the meaning of “cloning security information” but describes it as information that is used to program a key blank to prepare a duplicate of the master key. *See, e.g.*, Ex. 1001, 7:57-63 (“The cloning application 102 may communicate with the t/r device 10 to allow the antenna 40 to transmit the cloning security information 148 to the generically programmed duplicate key 50 to create a cloned duplicate key 50’.”); Ex. 1002 ¶¶61. Chies similarly describes processing the security information from the master key (e.g., the INCODE data) to prepare “OUTCODE” data used to program a blank transponder key. Ex. 1004, 7:29-8:9 (describing a process wherein “the INCODE is decrypted,” “the secret code is recognized and authenticated” such that “the single and sole secret code corresponding to the one contained in the microchip of the key 10 to be duplicated is acquired,” and “[t]he data processing centre 26

encrypts the corresponding secret code . . . into a second encryption form, which shall be defined as OUTCODE hereinafter.”), 8:21-34, Fig. 4.



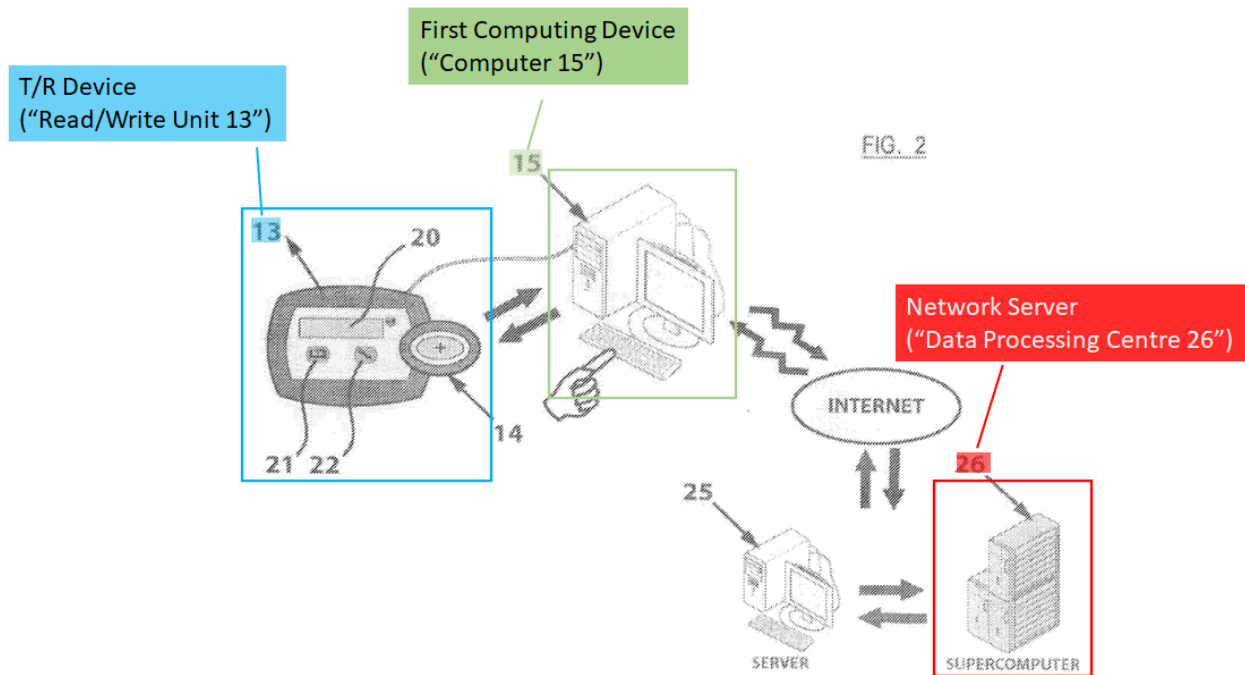
Chies thus discloses generating, by the network server, a cloning security information. Ex. 1002 ¶¶61-62.

1(f): communicating, by the network server, the cloning security information to the cloning application; and

Chies discloses a network server (e.g., data processing centre 26) communicating the cloning security information (e.g., OUTCODE data) to the cloning application (e.g., the application program of computer 15). Ex. 1004, 8:11-34. For example, data processing centre 26 sends the OUTCODE data to the read/write unit 13 “[v]ia the same telematic network” that was used to transmit the

key security information (e.g., INCODE) upstream to the data processing centre 26.

26. *Id.*, 8:11-12 (“Via the same telematic network, the data processing centre 26 sends the OUTCODE to the read/write unit 13 from which the related request had originated.”). This “telematic network” would have included each component of the network described in more detail for the upstream key information transmission process, including server 25, computer 15 (running the application program), and read/write unit 13. *Id.*, 6:15-7:27, Fig. 2; Ex. 1002 ¶63.



Because the transmission from the data processing centre 26 to the read/write unit 13 uses “the same telematic network,” a POSITA would have understood from Chies’ disclosure that data processing centre 26 would have communicated the OUTCODE data to the cloning application of computer 15,

which would have further communicated that data to the read/write unit 13.

Ex. 1004, 7:12-8:24; Ex. 1002 ¶64. This would have been the case at least because (as shown in Figure 2 above) computer 15 is connected to the peripheral read/write unit 13 via, e.g., USB, and is thus the network component enabling read/write unit 13 to transmit information over the network, including to/from data processing centre 26. Ex. 1004, 5:33-6:2; Ex. 1002 ¶64.

To the extent that Chies does not explicitly state that data processing centre 26 transmits the OUTCODE data to the application program of computer 15, a POSITA would have understood this to be the case (or at least would have found this obvious) based on Chies' disclosure of using computer 15 to provide network (e.g., Internet) access for peripheral read/write unit 13:

The peripheral read/write unit 13 is connected to a computer 15, e.g. via a serial interface RS232 or a Universal Serial Bus (USB). The computer 15 is interconnected with the Internet network and is located in proximity of the read/write unit 13. Installed in the same computer 15 there is an application program that is adapted to handle the flow of data coming in from the read/write unit 13.

Ex. 1004, 5:33-6:4; Ex. 1002 ¶65. Computer 15 would have therefore been an intermediate network component that receives the OUTCODE data from data

processing centre 26 and transmits that OUTCODE data to read/write unit 13 using the computer's application program. Ex. 1002 ¶65. The use of computers, such as computer 15, to transmit and receive information over the Internet for connected "peripheral" devices such as read/write unit 13 was also routine in the field and would have been well known in the art for decades, rendering this claim feature obvious in any event. Ex. 1002 ¶65.

It would have also been obvious to a POSITA that Chies' "application program" of computer 15 would have been the software on computer 15 receiving the cloning security information from the network server, as opposed to another program running on computer 15. Ex. 1002 ¶66. As noted above, Chies explains that the application program is computer 15's software interface with read/write unit 13 because the application program "is adapted to handle the flow of data coming in from the read/write unit 13." Ex. 1004, 5:33-6:4. Chies further states that the downstream information subsequently sent from data processing centre 26 to read/write unit 13 is sent "[v]ia the same telematic network" as the upstream transmissions, and a POSITA would have understood that the cloning security information would thus be sent to read/write unit 13 from data processing centre 26 via the application program of computer 15. *Id.*, 8:11-19; Ex. 1002 ¶66.

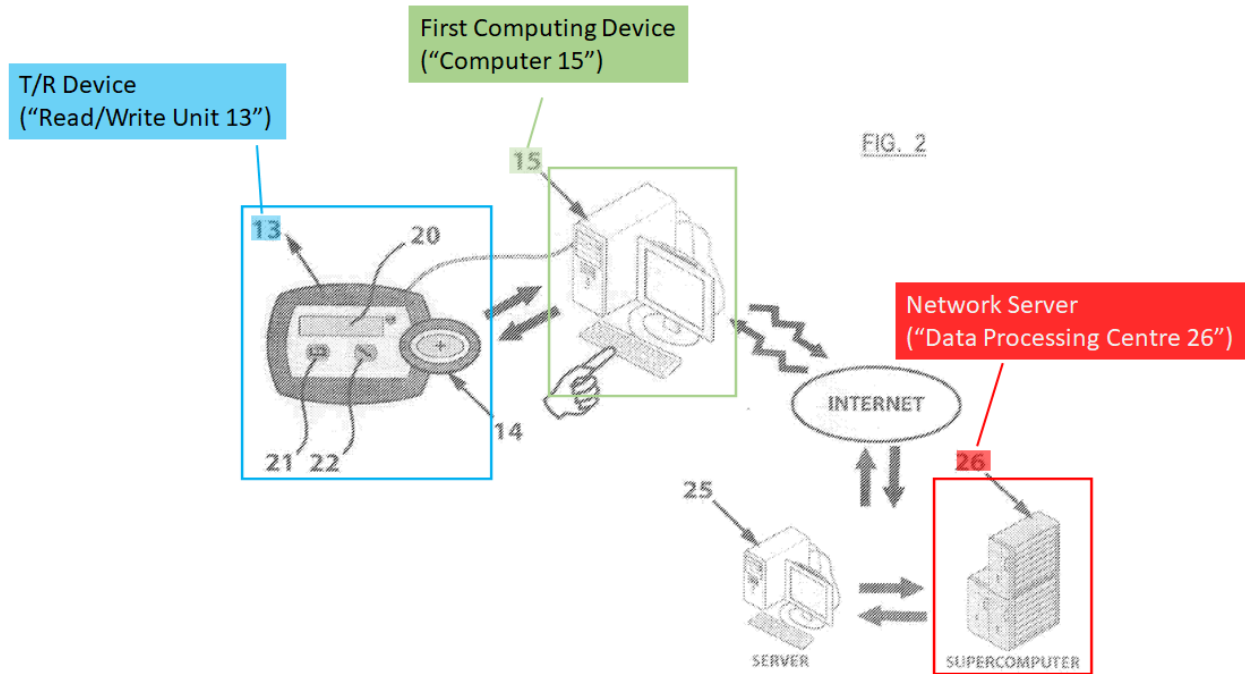
To the extent that Chies does not expressly state that the application program of computer 15 is used for downstream transmissions to read/write unit 13 as well

as upstream transmissions, a POSITA would have found it obvious to use the same program to send Chies' transponder key data in two directions (instead of one) for numerous reasons, including (1) improving the efficiency of computer 15 by only requiring the use of a single program for bidirectional transmissions, rather than using multiple programs; (2) reducing the overall complexity of the system, and thus the likelihood of errors in the transmission process; and (3) making the system as a whole easier to develop and deploy by reducing the number of programs of computer 15 that read/write unit 13 and data processing centre 26 would respectively interface with. Ex. 1002 ¶67. While no modification to Chies is necessary for the application program of computer 15 to perform this functionality, modifying Chies in this manner would in any event have required only routine skill, knowledge, and standard computer programming techniques, would have been a simple design choice for a POSITA (especially in view of the above-noted benefits of using the same program for this functionality), and would have yielded predictable results with a reasonable expectation of success, i.e., using a single application program for downstream transmissions over a data network in addition to managing upstream data transmissions. Ex. 1002 ¶67; *see KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416-417, 421 (2007); *Uber Techs., Inc. v. X One, Inc.*, 957 F.3d 1334, 1338-41 (Fed. Cir. 2020).

Chies therefore discloses, or at least renders obvious, communicating, by the network server, the cloning security information to the cloning application. Ex. 1002 ¶¶63-68.

1(g): transmitting, by the cloning application, the cloning security information to the t/r device to program an electronic access device of a generally programmable duplicate key with the cloning security information.

As discussed above for Claim 1(f), Chies discloses (or at least renders obvious) a network server (e.g., data processing centre 26) transmitting cloning security information (e.g., “OUTCODE” data) to a cloning application (e.g., the application program of computer 15). Ex. 1002 ¶¶63-69. Chies similarly discloses (or at least renders obvious) the application program of computer 15 transmitting the OUTCODE data to a t/r device (e.g., read/write unit 13) to program an electronic access device (e.g., “the microchip of the new blank key 30”) of a generally programmable duplicate key (e.g., blank key 30) with the OUTCODE data. Ex. 1004, 8:21-34. The network transmission path from the data processing centre 26 to the read/write unit 13 is “the same telematic network” used for upstream transmissions from the read/write unit 13 to the data processing centre 26, and that network includes computer 15 (running the application program), which transmits information to and from read/write unit 13. *Id.*, 5:33-6:2, Fig. 2; Ex. 1002 ¶69.



As with Claim 1(f), to the extent that Chies does not explicitly state that the application program of computer 15 transmits the OUTCODE data to the read/write unit 13, a POSITA would have understood this to be the case (or would have at least found this obvious) based on Chies' disclosure of using computer 15 to provide network (e.g., Internet) access for peripheral read/write unit 13. Ex. 1004, 5:33-6:2 ("The peripheral read/write unit 13 is connected to a computer 15, e.g. via a serial interface RS232 or a Universal Serial Bus (USB). The computer 15 is interconnected with the Internet network and is located in proximity of the read/write unit 13."); Ex. 1002 ¶70. Computer 15 would have therefore been an intermediate network component that receives the OUTCODE data from data processing centre 26 and transmits that OUTCODE data to

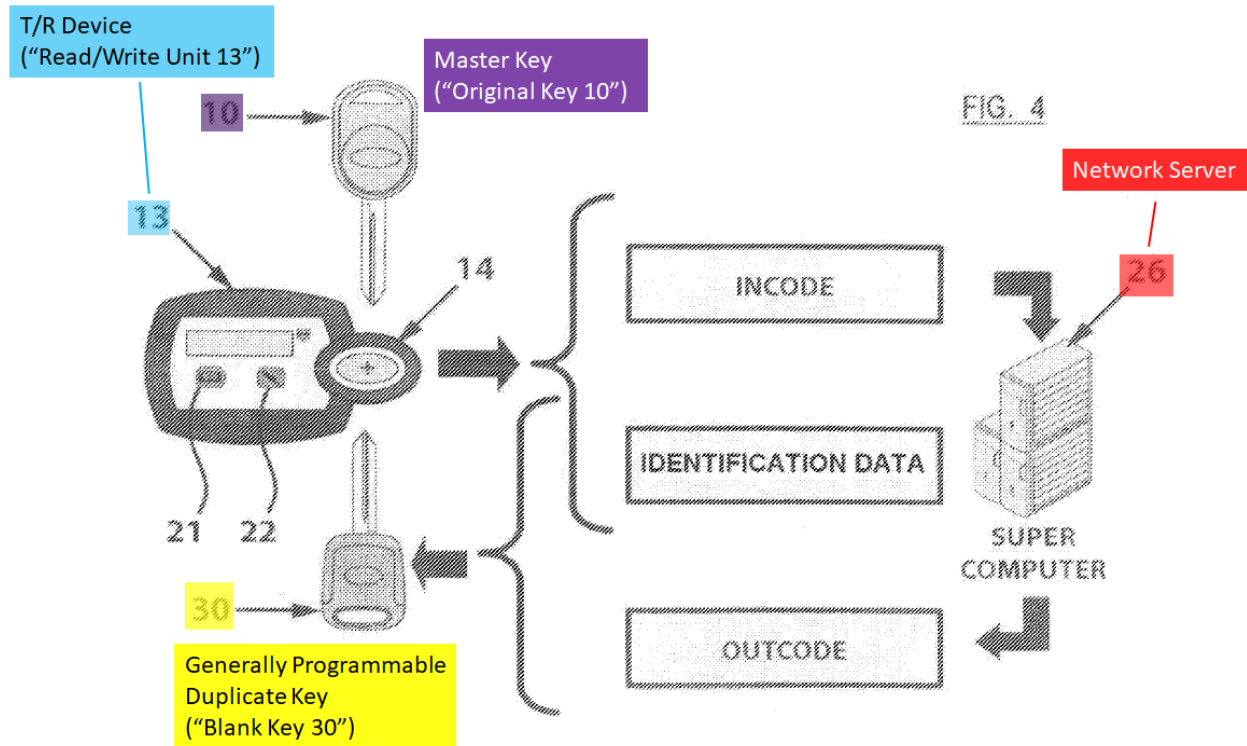
read/write unit 13 using the computer's application program. Ex. 1002 ¶70. The use of computers, such as computer 15, to transmit and receive information over the Internet for connected "peripheral" devices such as read/write unit 13 was also routine in the field and has been well known in the art for decades, rendering this claim feature obvious. Ex. 1002 ¶70. Moreover, as discussed for Claim 1(f) above, a POSITA would at least have found it obvious that the application program of computer 15 (as opposed to another program on the computer) would have managed transmitting the cloning security information to read/write unit 13. Ex. 1002 ¶¶63-68, 70.

After receiving the OUTCODE data, read/write unit 13 "transfers all identification data of [original key 10] into the microchip of the new blank key 30, wherein this operation is performed with the aid of the interactive write button 22." Ex. 1004, 8:21-29. The OUTCODE data is then "decrypted and definitively stored – along with the other identification data – solely inside the microchip of the blank key 30." *Id.*, 8:29-31. The blank key 30 is then "able to exactly emulate the functions of the configuration of the original key." *Id.*, 8:31-34.

Chies therefore discloses, or at least renders obvious, transmitting, by the cloning application, the cloning security information to the t/r device to program an electronic access device of a generally programmable duplicate key with the cloning security information. Ex. 1002 ¶¶69-72.

2. **Claim 3: The method of claim 1, further comprising: in response to communicating, by the cloning application, the security information for said master key to said network server, determining, by the network server, whether the security information is encrypted; and generating the cloning security information.**

Chies anticipates and/or renders obvious claim 1. Ex. 1002 ¶¶47-72. As discussed above for Claim 1(d), Chies discloses communicating, by a cloning application, security information for a master key to a network server. Ex. 1002 ¶¶58-60. Chies further discloses (or at least renders obvious), in response to this process, determining, by the network server (e.g., data processing centre 26), whether the security information (e.g., INCODE data) is encrypted, and generating the cloning security information (e.g., OUTCODE data). Ex. 1004, 7:29-8:9, Fig. 2. For example, data processing centre 26 decrypts the INCODE data (and thus determines whether it is encrypted when it does so) before generating the cloning security information (e.g., preparing the OUTCODE data). *Id.*; Ex. 1002 ¶73.



To the extent that Chies discloses decrypting the INCODE data but does not expressly state that it first determines whether that data is encrypted, a POSITA would have found it obvious to first determine whether data is encrypted at Chies' data processing centre 26 before performing decryption processing. Ex. 1002 ¶74. The process of characterizing whether information (such as transponder key information) is encrypted, known in the art as a form of "data typing," is a fundamental and routine aspect of information processing in the field of computer science that would have been known to a POSITA. Ex. 1002 ¶74. Determining whether data is encrypted before performing decryption processing—or before transmitting the data elsewhere for such processing—would have been beneficial to ensure the data is processed correctly. Ex. 1002 ¶74. For example, a POSITA

would have known that decrypting data that is not encrypted could corrupt that data, including potentially making the corrupted data unrecoverable. Ex. 1002 ¶¶74. Determining the data type prior to performing decryption processing on non-encrypted data would also have been expected to conserve computing resources, since decryption processing would not be necessary in those circumstances. Ex. 1002 ¶¶74. A POSITA would have had a reasonable expectation of success in determining the data type (i.e., whether the data is encrypted) before performing decryption processing, and doing so would have required only routine skill, knowledge, and standard computer programming techniques. Ex. 1002 ¶¶74; *see KSR*, 550 U.S. at 416-417, 421.

Chies thus discloses, or at least renders obvious, in response to communicating, by the cloning application, the security information for said master key to said network server, determining, by the network server, whether the security information is encrypted, and generating the cloning security information. Ex. 1002 ¶¶75.

C. Ground 3: Chies and Marsh Render Claims 2-6 Obvious.

1. Claim 2:

2(pre): “The method of claim 1, further comprising:”

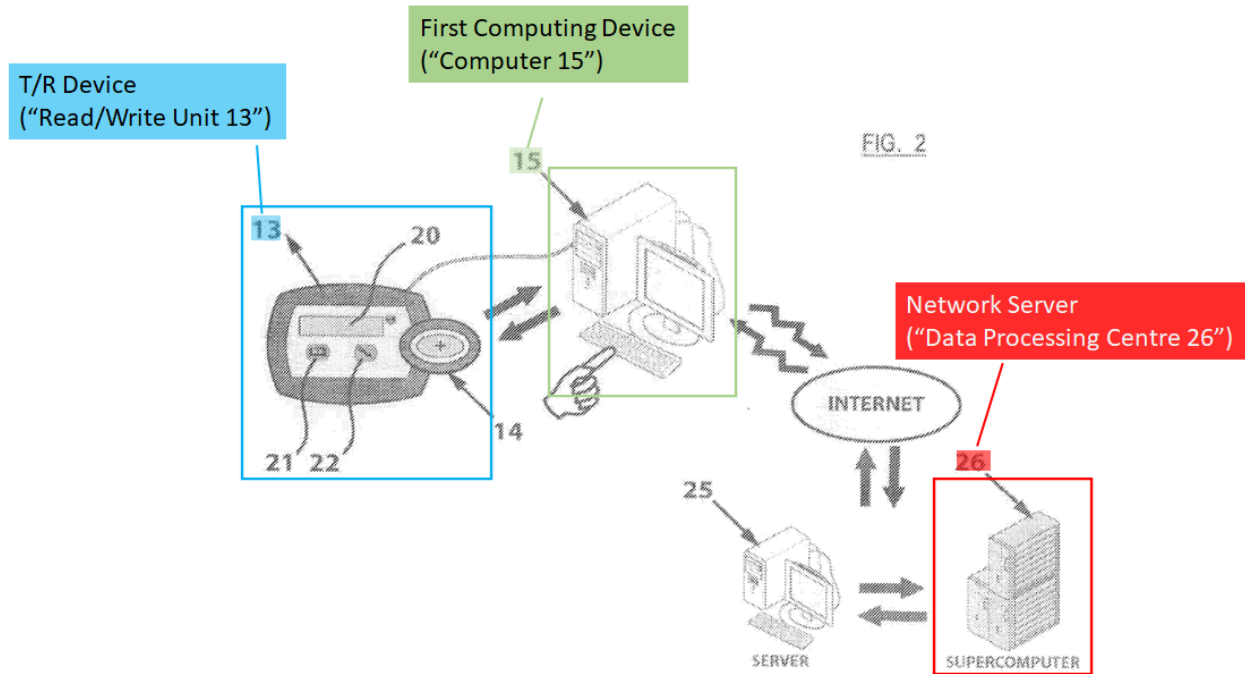
Chies anticipates and/or renders obvious claim 1. Ex. 1002 ¶¶47-72.

2(a): “in response to retrieving, by the t/r device, security information from said master key,”

As discussed above for Claim 1(c), Chies discloses (or at least renders obvious) using a t/r device to retrieve security information from a master key. Ex. 1002 ¶¶55-57.

2(b): “determining, by the cloning application, whether the security information is encrypted and”

78. A POSITA would have found it obvious, in view of the disclosures of Chies and Marsh, to determine whether the security information (e.g., the INCODE data) is encrypted by Chies’ cloning application (e.g., the application program of computer 15) before performing decryption processing. Ex. 1002 ¶78. For example, Chies’ application program communicates the INCODE data of a master key (e.g., key 10) to a network server (e.g., data processing centre 26). Ex. 1004, 6:15-7:31, Fig. 2.



Marsh discloses a network server (e.g., server 1310) that is remote from a computer running a cloning application (e.g., software on kiosk 200 that transmits the key information to server 1310). *See* Ex. 1005, 17:51-55 (kiosk 200 transmits key information to server 1310), 19:54-58 (kiosks 200 “can include any of a general purpose device such as a computer”), 24:34-43 (noting that kiosk 200 is an example of “a computing device executing process 1800,” as shown in Fig. 18), 26:30-53 (describing computer programs “such as . . . a computer application”), Fig. 13. Marsh further discloses that server 1310 may, upon receiving the information related to the transponder key, “*determine whether the information received from the transponder key is encrypted and/or can decrypt the information received from the transponder key.*” *Id.*, 25:26-32 (emphasis added); Ex. 1002 ¶79.

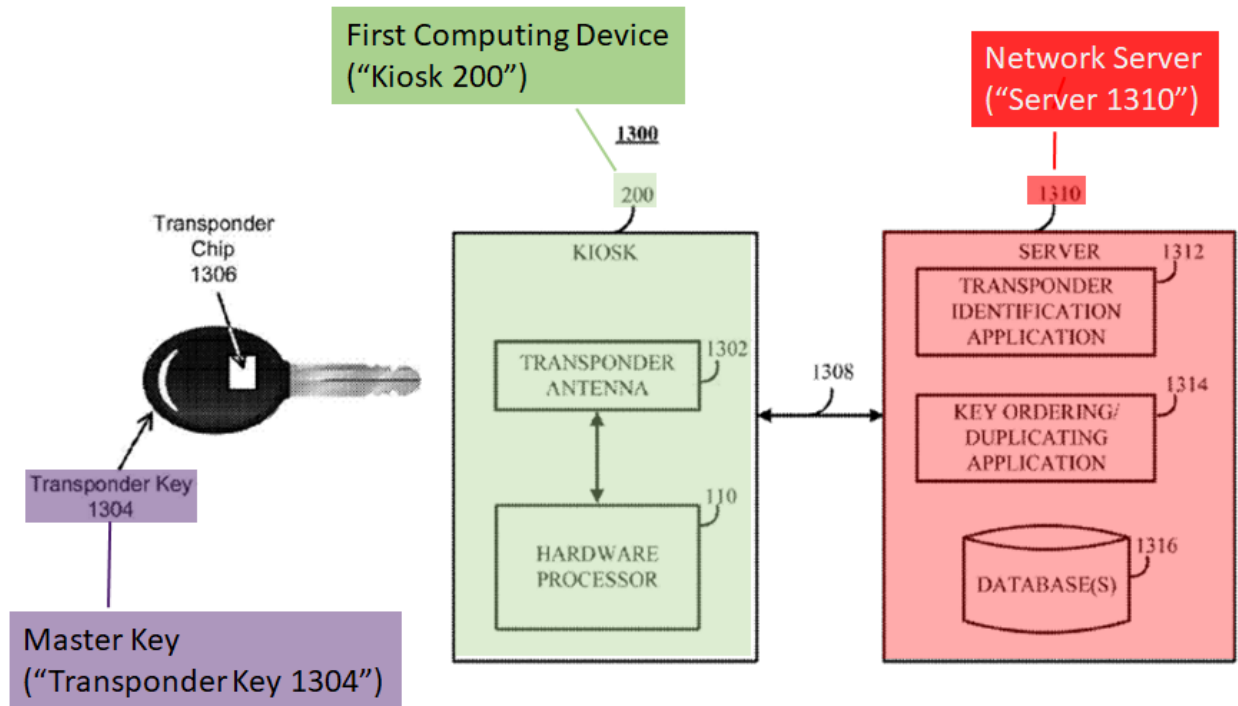


FIG. 13

A POSITA considering Chies in view of Marsh's disclosure of "determin[ing] whether the information received from the transponder key is encrypted" would have found it obvious to similarly determine whether Chies' transponder key information is encrypted at Chies' application program before performing decryption processing (or before transmitting the transponder key information to a remote server to perform such processing). Ex. 1002 ¶80. For example, a POSITA would have found it obvious to first determine whether the security information read from the master key is encrypted at Chies' application program prior to transmitting that information to a remote server (e.g., data processing centre 26) for decryption processing. Ex. 1002 ¶80.

The process of characterizing whether information (such as transponder key information) is encrypted, known in the art as a form of “data typing,” is a fundamental and routine aspect of information processing in the field of computer science that would have been known to a POSITA. Ex. 1002 ¶81. Determining whether data is encrypted before performing decryption processing—or before transmitting the data elsewhere for such processing—would have been beneficial to ensure the data is processed correctly. Ex. 1002 ¶81. For example, a POSITA would have known that decrypting data that is not encrypted could corrupt that data, including potentially making the corrupted data unrecoverable. Ex. 1002 ¶81. Determining the data type prior to performing decryption processing on non-encrypted data would also have been expected to conserve computing resources, since decryption processing would not be necessary in those circumstances. Ex. 1002 ¶81. A POSITA would have had a reasonable expectation of success in determining the data type (i.e., whether the data is encrypted) before performing decryption processing, and doing so would have required only routine skill, knowledge, and standard computer programming techniques. Ex. 1002 ¶81; *see KSR*, 550 U.S. at 416-417, 421.

A POSITA having this fundamental knowledge of decryption processing would have understood that it may not be necessary to perform such processing in Chies’ system, depending on whether the key information received by read/write

unit 13 is encrypted. Ex. 1002 ¶82. Chies states that it assumes, for purposes of its disclosure, that the transponder key information is encrypted and does not explicitly discuss an alternative where the key information is not encrypted. Ex. 1004, 6:30-7:10 (“*In the assumption that the key 10 is of the type with a secret (encrypted) code*, the read/write unit concurrently performs an inquiry operation to query the key 10”) (emphasis added); Ex. 1002 ¶82. But a POSITA would have understood that, if Chies’ application program of computer 15 determined that the received transponder key information was not encrypted (as it would have been obvious to do), then it would not be necessary for the application program to transmit the transponder key data to data processing centre 26 for decryption processing. Ex. 1002 ¶82. Rather, a POSITA would have understood that it would be beneficial for the application program to instead send the non-encrypted key information back to read/write unit 13 (after performing this encryption check) to copy the non-encrypted data to a transponder key blank in a simple and routine data copying operation without consuming computing resources to unnecessarily transmit the data to data processing centre 26, thus reducing the application program’s use of network bandwidth. Ex. 1002 ¶82. Modifying Chies’ system to operate in this manner would have required only routine skill, knowledge, and standard computer programming techniques, including routine read/write operations for duplicating non-encrypted data, and a POSITA would have had a

reasonable expectation of success when doing so in view of the POSITA's
aforementioned knowledge of decryption processing. Ex. 1002 ¶82; *see KSR*, 550
U.S. at 416-417, 421.

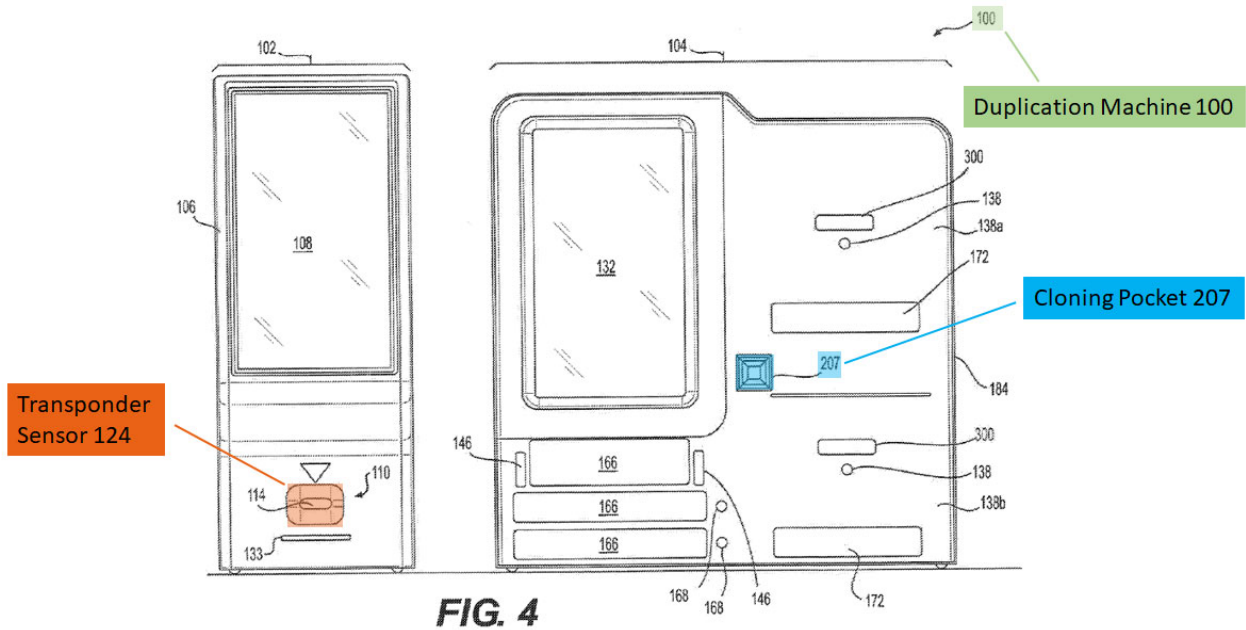
2(c): “generating the cloning security information”

If this clause of the claim term is interpreted such that the “generating the
cloning security information” occurs at the claimed network server, then as
discussed above for Claims 1(e) and 3, Chies alone discloses that interpretation.
Ex. 1002 ¶¶61-62, 73-75, 83. For example, Chies describes performing decryption
processing on the encrypted INCODE data at data processing centre 26, thus
generating cloning security information (e.g., OUTCODE data). Ex. 1004, 7:29-
8:9.

If this clause is alternatively interpreted to require that the cloning
application (running on the first computing device, per Claim 1(b)) generates the
cloning security information, a POSITA would have found that obvious based on
the disclosures of Chies and Marsh. Ex. 1002 ¶84. As discussed above, Chies
discloses a cloning application (e.g., the application program of computer 15). Ex.
1004, 5:33-6:4, 7:12-19; Ex. 1002 ¶85. Marsh discloses a key duplication system
including a network server (e.g., server 1310) that determines whether the master
transponder key's security information is encrypted and that can decrypt that
information. Ex. 1005, 25:26-32; Ex. 1002 ¶85. Marsh further explains that its key

duplication hardware and software may be deployed in a wide variety of locations and configurations, including as “client-side software” and “client-side hardware” for “the mechanisms described herein,” which include its server-side decryption processing systems. Ex. 1005, 26:30-34; Ex. 1002 ¶85.

A POSITA would understand, from Marsh’s broad disclosure regarding the placement of its various computing devices and processes as either “client-side” (i.e., near the master key being duplicated) or “server-side” (i.e., in a remote server such as server 1310), that the exemplary decryption processing systems of Marsh’s server 1310 could alternatively be deployed client side, e.g., in kiosk 200. Ex. 1002 ¶85. Indeed, client-side key duplication systems were known in the art. Ex. 1002 ¶86. For example, Gerlings describes a system for duplicating transponder keys locally at a kiosk (i.e., without an express use of a remote database/server) as shown in annotated Figure 4 below, wherein key duplication machine 100 (**green** below) scans a transponder key at transponder sensor 124 (**orange** below) to program a duplicate transponder key at cloning pocket 207 (**blue** below). *See* Ex. 1007 ¶¶50, 82, 88, 97-98; Ex. 1002 ¶86.



A POSITA would have understood several benefits of performing decryption processing (and generating the information for programming into a blank transponder key) in a client-side application like the application program of computer 15, such as to (1) improve the security of the system by maintaining sensitive key data locally (i.e., in proximity to a user and the key being duplicated); (2) reduce the use of network resources by eliminating the need to transmit encrypted information from kiosk 200 to server 1310 in situations where kiosk 200 is able to decrypt and duplicate the key information; (3) reduce the complexity of the key duplication system by consolidating processing resources in one place (e.g., within kiosk 200), rather than using a distributed system (including remote servers) with multiple potential points of processing delay or failure; and (4)

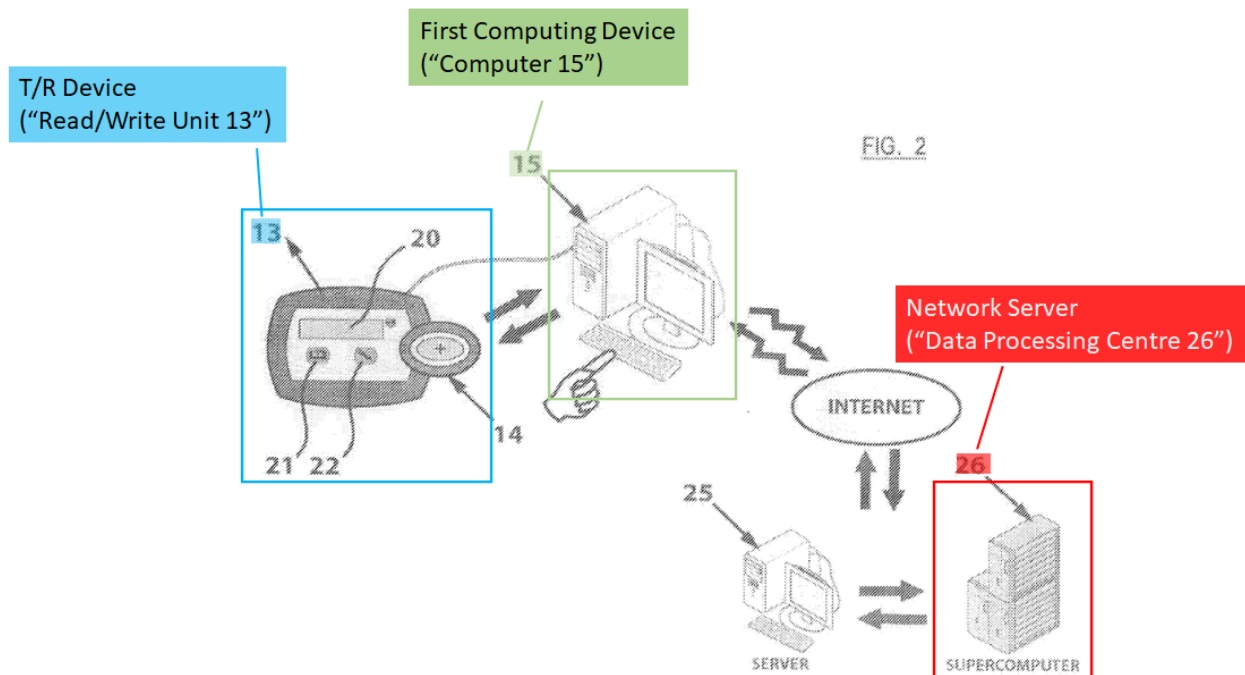
improve the response speed of the system (and the speed of overall key duplication for a customer) by eliminating unnecessary network components from the key duplication process, especially when duplicating transponder keys where the kiosk 200 is able to decrypt and duplicate the key information. Ex. 1002 ¶87.

In view of Marsh's disclosure, a POSITA would have found it obvious to modify Chies to incorporate a client-side decryption engine (e.g., the decryption system of data processing centre 26) in the application program of computer 15 to obtain the aforementioned benefits of client-side data decryption and generation of blank transponder key information. Ex. 1002 ¶88. A POSITA would have had a reasonable expectation of success in doing so because this modification would have required only routine skill, knowledge, and standard computer programming and manufacturing techniques, and would have been a simple design choice within the skill of a POSITA between two known alternatives (i.e., either performing the transponder data decryption/processing in a client-side system or a server-side system). Ex. 1002 ¶88; *see KSR*, 550 U.S. at 416-417, 421; *Uber*, 957 F.3d at 1338-41.

Chies in combination with Marsh thus renders obvious, in response to retrieving, by the t/r device, security information from said master key, determining, by the cloning application, whether the security information is encrypted and generating the cloning security information. Ex. 1002 ¶¶76-89.

2. **Claim 3: The method of claim 1, further comprising: in response to communicating, by the cloning application, the security information for said master key to said network server, determining, by the network server, whether the security information is encrypted; and generating the cloning security information.**

Chies anticipates and/or renders obvious claim 1. Ex. 1002 ¶¶47-72. As discussed above in for Claim 1(d), Chies discloses communicating, by a cloning application (running of computer 15), security information for a master key to a network server. Ex. 1004, 6:15-7:31, Fig. 2; Ex. 1002 ¶¶58-60.



Chies further discloses, in response to this process, determining, by the network server (e.g., data processing centre 26) whether the security information (e.g., INCODE data) is encrypted, and generating the cloning security information (e.g., OUTCODE data; *see* Claim 1(e) above). Ex. 1004, 7:29-8:9; Ex. 1002 ¶¶61-

62. For example, data processing centre 26 decrypts the INCODE data (and thus determines whether it is encrypted when it does so) before preparing the OUTCODE data. *Id.*; Ex. 1002 ¶91.

As discussed above for Claim 2, to the extent that Chies discloses decrypting the INCODE data but does not expressly state that data processing centre 26 first determines whether that data is encrypted, a POSITA would have found it obvious to first determine whether data is encrypted before performing decryption processing in view of the disclosure of Marsh. Ex. 1002 ¶¶76-89. In particular, Marsh discloses a network server (e.g., server 1310) that is remote from a computer running a cloning application (e.g., software on kiosk 200 that transmits the key information to server 1310). *See* Ex. 1005, 17:51-55 (kiosk 200 transmits key information to server 1310), 19:54-58 (kiosks 200 “can include any of a general purpose device such as a computer”), 24:34-43 (noting that kiosk 200 is an example of “a computing device executing process 1800,” as shown in Fig. 18), 26:30-53 (describing computer programs “such as . . . a computer application”). Marsh further discloses that server 1310 may, upon receiving the information related to the transponder key, “determine whether the information received from the transponder key is encrypted and/or can decrypt the information received from the transponder key.” *Id.*, 25:26-32; Ex. 1002 ¶92.

A POSITA considering Chies in view of Marsh’s disclosure of “determin[ing] whether the information received from the transponder key is encrypted” would have found it obvious to similarly determine whether Chies’ transponder key is encrypted at the network server (e.g., Chies’ data processing centre 26) before performing decryption processing. Ex. 1002 ¶¶93. Determining whether data is encrypted before performing decryption processing—or before transmitting the data elsewhere for such processing—would have been beneficial to ensure the data is processed correctly. Ex. 1002 ¶¶93. For example, a POSITA would have known that decrypting data that is not encrypted could corrupt that data, including potentially making the corrupted data unrecoverable. Ex. 1002 ¶¶93. Determining the data type prior to performing decryption processing on non-encrypted data would also have been expected to conserve computing resources, since decryption processing would not be necessary in those circumstances. Ex. 1002 ¶¶93. A POSITA would have had a reasonable expectation of success in determining the data type (i.e., whether the data is encrypted) before performing decryption processing, and doing so would have required only routine skill, knowledge, and standard computer programming techniques. Ex. 1002 ¶¶93; *see KSR*, 550 U.S. at 416-417, 421.

Chies in combination with Marsh thus renders obvious, in response to communicating, by the cloning application, the security information for said

master key to said network server, determining, by the network server, whether the security information is encrypted, and generating the cloning security information.

Ex. 1002 ¶¶90-94.

3. Claim 4:

4(pre): The method of claim 1, further comprising:

Chies anticipates and/or renders obvious claim 1. Ex. 1002 ¶¶47-72, 95.

4(a): capturing at least one image of a blade of said master key,

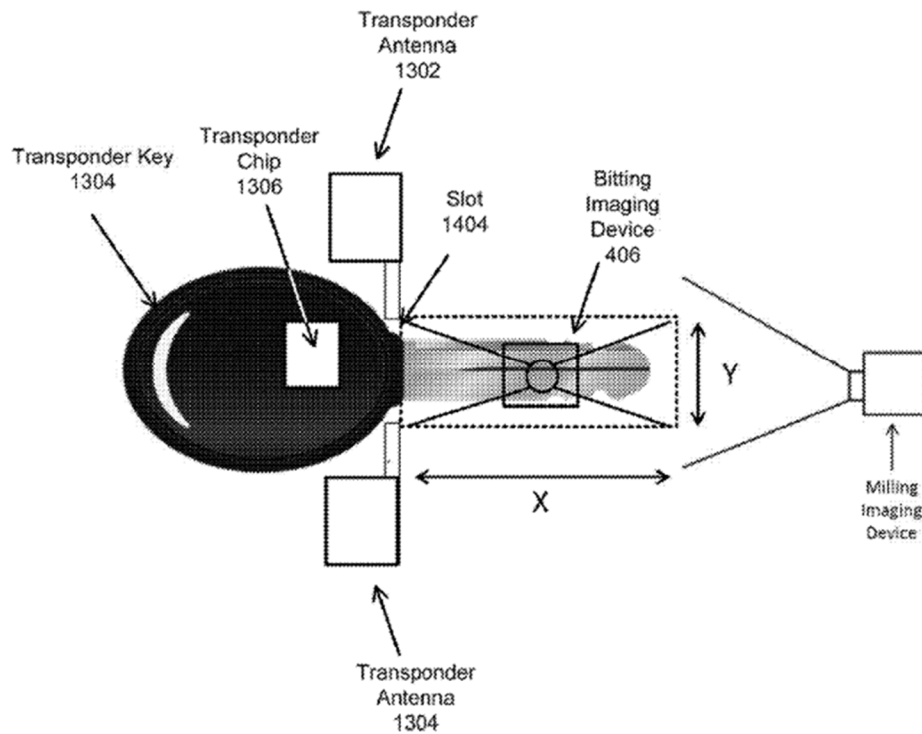
Chies does not explicitly disclose capturing at least one image of a blade of said master key. Ex. 1002 ¶96.

Marsh discloses systems and methods of duplicating keys, including several embodiments relating to imaging the blade of a key in order to duplicate it. Ex. 1002 ¶97. For example, Marsh discloses key detector 106, which “can be any suitable mechanism for detecting the biting pattern and/or the blank type of a key,” including optical technologies (e.g., cameras). Ex. 1005, 5:32-33; Ex. 1002 ¶97. Marsh also describes “imaging devices 406 and 408,” which “can be used to optically detect a biting pattern and a key blank type of the key,” including by capturing images of the key. Ex. 1005, 13:41-50. For transponder keys, in particular, Marsh discloses obtaining images of the key where the:

image data can include a shape of the key head, one or more logos associated with the transponder key, a shape

and/or position of the shaft of the transponder key (if the transponder key includes a shaft), a biting pattern of the transponder key (if the transponder key includes a biting pattern), an overall shape of the transponder key, textual information associated with the transponder key and/or any other suitable information.

Id., 22:64-23:10; *see also id.*, 2:30-37 (describing “receiving an image of the transponder key captured by an image sensor included in the key scanner; determining geometric information about the transponder key based on an image of the transponder key captured by the image sensor; and causing the geometric information about the transponder key to be used to create the duplicate transponder key.”), 16:59-65, 18:39-67 (describing obtaining the “geometric properties of the key (e.g., using detector(s) 106)”), Fig. 14; Ex. 1002 ¶97.



A POSITA would have been motivated to modify Chies to incorporate the key blade imaging systems and methods disclosed by Marsh to expand the capabilities of the Chies system, such as by enabling Chies' system to additionally duplicate the blade of a master key in addition to the transponder data of the key. Ex. 1002 ¶98. A POSITA would have understood that doing so would allow for a duplicate key to include the characteristics of the master key's blade in addition to the transponder data, thereby allowing the duplicate transponder key to be a more complete duplicate of the master transponder key. Ex. 1002 ¶98. Duplicating the blade of the master key in this manner would enable the duplicate key to provide access to systems or devices that may not otherwise be accessible using only the transponder data, such as an ignition to a car engine requiring insertion of the key

blade for activation. Ex. 1002 ¶98. The concept of imaging and duplicating key blades has been known in the key duplication field for decades, and modifying Chies in this manner would have required only routine skill, knowledge, and standard manufacturing techniques, and would have yielded predictable results with a reasonable expectation of success, i.e., having a system capable of duplicating both the transponder data of a transponder key as well as the blade of the transponder key. Ex. 1002 ¶98; *see KSR*, 550 U.S. at 416-17, 421.

The combination of Chies and Marsh thus renders obvious capturing at least one image of a blade of said master key. Ex. 1002 ¶¶96-99.

4(b): communicating said at least one image of said blade to said network server,

Chies does not explicitly disclose communicating at least one image of a key blade to a network server. Ex. 1002 ¶100. Marsh discloses communicating the captured images of a transponder key's blade to a network server. Ex. 1002 ¶101. For example, in addition to obtaining images of a transponder key as part of process 1800 for duplicating the transponder key (e.g., Ex. 1005, 22:64-23:10), Marsh further discloses sending “geometric information about a shaft portion of the transponder key” to a network server (e.g., server 1310) from kiosk 200 to duplicate the transponder key. Ex. 1005, 2:30-37, 16:59-65, 18:2-67, 20:59-67, 25:33-47, Fig. 13.

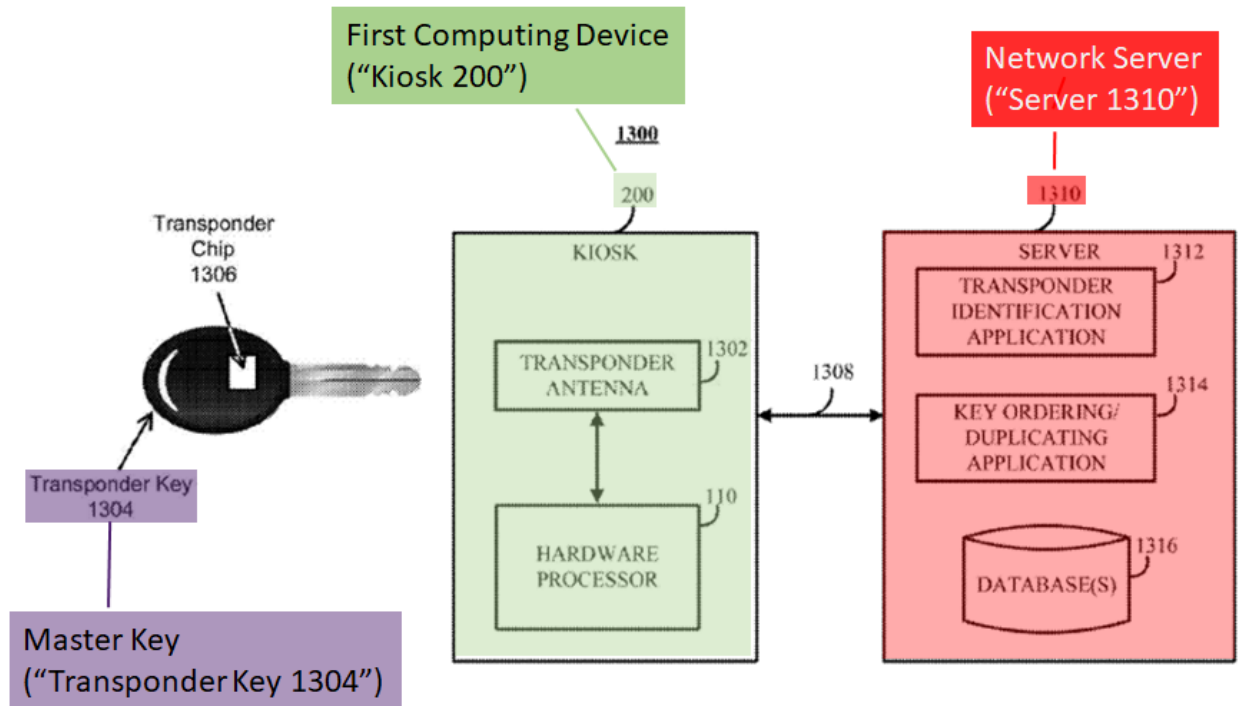


FIG. 13

A POSITA would have understood that Marsh’s disclosure of sending the image data (including the key’s “geometric information”) to a network server would have included transmitting (i.e., communicating) the images of the key blade used to duplicate the key to server 1310 for further processing. Ex. 1002

¶102. A POSITA would have been motivated to implement Marsh’s capabilities of communicating at least one image of the key blade to the network server into Chies’ system for the same reasons described above for Claim 4(a). Ex. 1002 ¶¶96-99, 102. A POSITA would have had a reasonable expectation of success in doing so, as this would have required only routine skill, knowledge, and standard

computer programming techniques. Ex. 1002 ¶102; *KSR*, 550 U.S. at 416-417, 421.

The combination of Chies and Marsh thus renders obvious communicating said at least one image of said blade to said network server. Ex. 1002 ¶¶100-103.

4(c): cutting a duplicate blade of a generally programmable duplicate key, and

Chies does not explicitly disclose cutting a duplicate blade of a generally programmable duplicate key. Ex. 1002 ¶104. Marsh discloses cutting a blade of a generally programmable duplicate key (e.g., a transponder key blank) to create a duplicate of a master transponder key. Ex. 1002 ¶105. For example, Marsh describes key cutting and cleaning mechanisms used to cut a key blank. Ex. 1005, 8:6-43, 10:31-40 (describing using a key cutting mechanism “to cut the key according to the detected biting pattern and then clean the key to remove burrs, etc.”), 12:32-41. Marsh further describes cutting a key blank for a transponder key “based on geometric information included in the key information.” *Id.*, 18:27-30. Marsh also describes providing the duplicate key to a customer from a remote location by allowing the customer to “request a physical copy via mail order,” as well as to “make a physical copy with any suitable key duplication hardware” (i.e., cutting a duplicate blade of a generally programmable duplicate key at a remote location before mailing it to a customer). Ex. 1005, 15:10-27; Ex. 1002 ¶105.

A POSITA would have been motivated to implement Marsh's capabilities of cutting a duplicate blade of a generally programmable duplicate key into Chies' system for the same reasons described above for Claim 4(a). Ex. 1002 ¶¶96-99, 106. A POSITA would have had a reasonable expectation of success in doing so, as this would have required only routine skill, knowledge, and standard computer programming and/or manufacturing techniques. Ex. 1002 ¶106; *see KSR*, 550 U.S. at 416-417, 421.

The combination of Chies and Marsh thus renders obvious cutting a duplicate blade of a generally programmable duplicate key. Ex. 1002 ¶¶104-107.

4(d): providing said generally programmable duplicate key to said customer.

Chies does not explicitly disclose providing a generally programmable duplicate key to a customer after cutting the blade of the key blank. Ex. 1002 ¶108. Marsh describes, after cutting the blade of a generally programmable duplicate key (e.g., transponder key blank) and programming a transponder chip within the key blank, causing the "the key to be dispensed to a user. For example, the hardware processor can control the key cutting and cleaning mechanism 116 to drop the key in the key dispensing chute." Ex. 1005, 10:41-44, 13:1-4, 25:48-52 (describing conducting process 1800 for duplicating a transponder key in conjunction with process 300 for duplicating a key, including cutting the blade of the key blank),

Fig. 2 (see “Key Dispensing Chute” below); Ex. 1002 ¶109. In addition to dispensing a physical copy of the duplicate key at a kiosk, Marsh also describes providing the duplicate key to a customer from a remote location by allowing the customer to “request a physical copy via mail order,” as well as to “make a physical copy with any suitable key duplication hardware.” Ex. 1005, 15:10-27; Ex. 1002 ¶109.

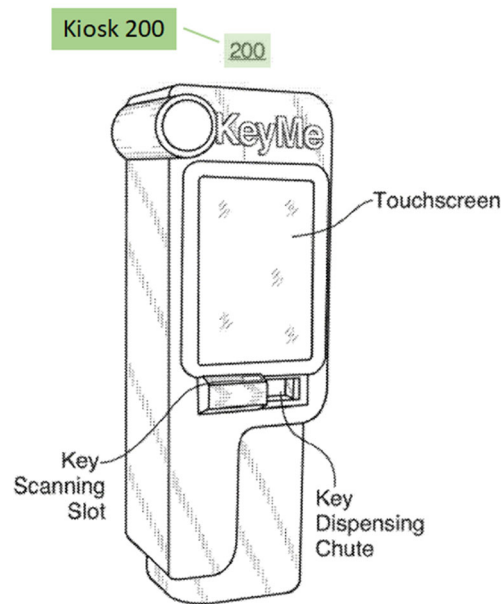


FIG. 2

A POSITA would have been motivated to implement Marsh’s capabilities of providing the generally programmable duplicate key to a customer (e.g., a user of Marsh’s kiosk 200) after cutting the blade of the key blank into Chies’ system for the same reasons described above for Claim 4(a). Ex. 1002 ¶¶96-99, 110. A POSITA would have had a reasonable expectation of success in doing so, as this

would have required only routine skill, knowledge, and standard computer programming and/or manufacturing techniques. Ex. 1002 ¶110; *see KSR*, 550 U.S. at 416-417, 421. The combination of Chies and Marsh thus renders obvious providing the generally programmable duplicate key to a customer. Ex. 1002 ¶¶108-110.

4. **Claim 5: The method of claim 1, further comprising:
placing said generally programmable duplicate key in
proximity with said vehicle, sampling communications
between said generically programmable duplicate key and
said vehicle to generate authentication sample data.**

Chies anticipates and/or renders obvious claim 1. Ex. 1002 ¶¶47-72, 111. Chies does not explicitly disclose placing a generally programmable duplicate key in proximity with a vehicle and sampling communications between the generally programmable duplicate key and the vehicle to generate authentication sample data. Ex. 1002 ¶111.

Marsh discloses placing a transponder key in proximity with a vehicle in order to obtain a responsive signal from the transponder key. Ex. 1002 ¶112. For example, Marsh discloses the use of a “portable scanning device” associated with kiosk 200 to be used with a “device that emits the signal that includes the particular information (e.g., the automobile corresponding to the transponder key).” Ex. 1005, 24:34-43. The portable scanning device “can capture one or more signals emitted by the transponder by the transponder key responsive to the signal emitted

by, for example, the automobile.” *Id.*, 24:44-47. The portable scanning device “can include an input device (e.g., a button), and process 1800 can instruct a user to operate the input device (e.g., by pressing the button) when the user has brought the transponder key into the automobile and/or performed any other suitable actions (such as operating an ignition of the automobile).” *Id.*, 24:47-53, Fig. 18.

A POSITA would have understood that Marsh’s disclosure describes placing a transponder key in proximity with a vehicle, for example, to sample communications between the transponder key and the vehicle to generate authentication sample data, such as when a transponder key must first receive a signal emitted by the vehicle before emitting information that can be used to create a duplicate transponder key:

[I]n the case of an automobile key using a passive transponder chip, the mechanisms described herein for duplicating transponder keys and managing key information thereof can cause a signal to be emitted that, in turn, causes the passive transponder chip of the automobile key to emit a responsive signal that is required by the automobile in order to allow the automobile to be started and/or turned on. This responsive signal can be used to identify the properties and/or programming of a transponder chip to be used to create a duplicate of the automobile key.

Ex. 1005, 16:8-19, 24:7-33; Ex. 1002 ¶113. Using the same rationale taught by Marsh, a POSITA would have found it obvious to place a generally programmable duplicate key (e.g., a transponder key blank) in proximity with a vehicle to generate similar authentication sample data, such as to determine whether the key blank is an appropriate model and type for the vehicle at issue and to obtain the sample data emitted from the key blank. Ex. 1002 ¶113. Sampling communications between a transponder key and a vehicle in this manner was routine and well-known in the art, and a POSITA would have found it obvious to practice the method of sampling communications between a transponder key and a vehicle (as taught by Marsh) in the key duplication process taught by Chies in order to obtain the same benefits taught by Marsh, i.e., to generate responsive data from the transponder in proximity to the vehicle that is useful to the key duplication process. Ex. 1002 ¶113. A POSITA would have had a reasonable expectation of success in doing so with the blank transponder key, as this would have required only routine skill, knowledge, and techniques already taught by the prior art. Ex. 1002 ¶113; *see KSR*, 550 U.S. at 416-417, 421.

The combination of Chies and Marsh thus renders obvious placing said generally programmable duplicate key in proximity with said vehicle, sampling communications between said generically programmable duplicate key and said vehicle to generate authentication sample data. Ex. 1002 ¶¶111-114.

5. Independent Claim 6

6(pre): A vehicle access device duplication system comprising:

If the preamble is limiting, Chies discloses a vehicle access device duplication system. Ex. 1004, 1:10-17, 4:26-29; Ex. 1002 ¶115.

6(a): a non-transitory computer-readable storage medium storing executing instructions that, when executed, cause a cloning application to perform steps comprising:

Chies discloses a computer (e.g., computer 15) that includes a cloning application (e.g., the “application program”) performing steps for duplicating a transponder key. Ex. 1004, 5:33-6:28 (“Installed in the same computer 15 there is an application program that is adapted to handle the flow of data coming in from the read/write unit 13.”), 7:12-19 (“The read/write unit 13 transmits the INCODE . . . to the computer connected thereto. The computer 15, as duly provided with the application program, receives such information and sends it to the serving computer or server 25.”); Ex. 1002 ¶116. While Chies does not expressly describe a storage medium within computer 15, a POSITA would have understood that computer 15 would include a readable storage medium for permanent (i.e., non-transitory) storage of programs and data, such as a hard disk drive storing the “application program” and any associated computer code allowing the computer 15 to execute instructions associated with the application

program. Ex. 1002 ¶116. Such storage devices are ubiquitous in computers and have been used for decades, and a POSITA would have interpreted Chies' computer 15 as including such a storage medium for storing and executing the computer code for the application program. Ex. 1002 ¶116.

To the extent that Chies lacks express details regarding the storage of computer 15, the use of a non-transitory computer-readable storage medium that stores instructions that, when executed, cause an application to perform certain steps would have been obvious in view of Marsh. Ex. 1002 ¶117. Marsh's kiosk 200 includes a computer containing a non-transitory computer-readable storage medium (e.g., the computer memory within the kiosk such as a hard disk or other computer-readable media). Ex. 1005, 19:54-20:18 (kiosks 200 "can include any of a general purpose device such as a computer," which may include "any suitable components such as a hardware processor" and "memory"), 20:47-58, 26:54-67 (describing "computer readable media [that] can be used for storing instructions for performing the processes described herein" as including "non-transitory computer-readable media" such as "magnetic media (such as hard disks)," "optical media," and "semiconductor media"). This storage medium in Marsh's kiosk 200 stores executing instructions that, when executed, cause a cloning application to perform certain steps. Ex. 1005, 20:47-67 (describing "a non-transitory computer-readable medium[] for storing a computer program for controlling hardware processor

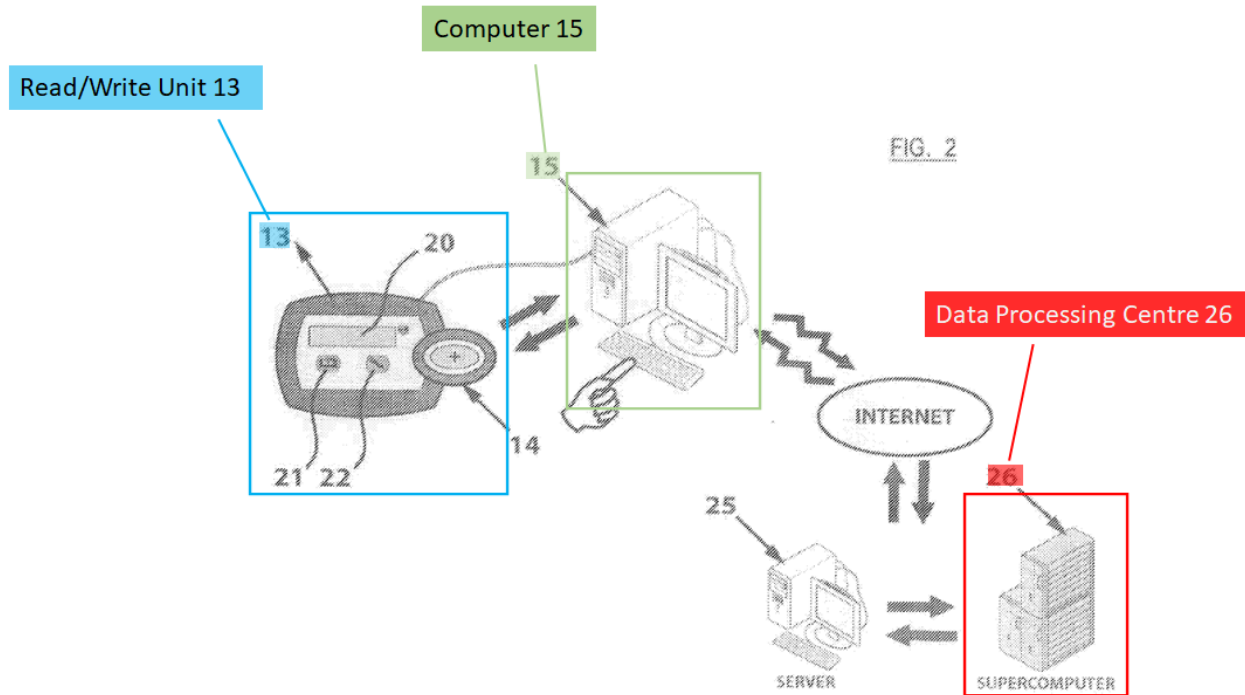
1702,” wherein “[h]ardware processor 1702 can use the computer program to execute the mechanisms described herein for duplicating keys and/or duplicating transponder keys and managing the key information thereof”), 24:34-61 (kiosk 200 is a “computing device executing process 1800” for duplicating a transponder key), 26:30-53 (describing the use of a computer program “that causes a processor (such as hardware processor 110, hardware processor 1702 and/or hardware processor 1722) to execute the mechanisms described herein,” such as a computer program “written in a programming language recognizable by kiosk 200”), Fig. 13.

To the extent it would have been necessary to modify Chies’ computer 15 to include a non-transitory computer-readable storage medium such as Marsh’s, a POSITA would have been motivated to do so to allow computer 15 to store the application program in permanent storage, thereby allowing repeated use of the application program, and would have had a reasonable likelihood of success in doing so given that the use of such storage mediums (and storing programs on such storage mediums) was routine and well-known in the field. Ex. 1002 ¶118; *see KSR*, 550 U.S. at 416-417, 421.

Chies alone, or in combination with Marsh, thus renders obvious a non-transitory computer-readable storage medium storing executing instructions that, when executed, cause a cloning application to perform steps. Ex. 1002 ¶¶116-119.

6(b): determining that a first device of a customer is communicating with a transmitter/receiver device (t/r device), the t/r device including an antenna ring for wirelessly communicating with an access device for a vehicle;

Chies discloses a t/r device (e.g., read/write unit 13) that wirelessly communicates with an access device for a vehicle (e.g., key 10). Ex. 1002 ¶120. For example, Chies discloses duplicating original key 10 by inserting it into a read/write unit 13 (**blue** in annotated Figure 2 below) and establishing wireless communication via the antenna of the read/write unit 13. Ex. 1004, 4:26-5:2, Fig. 2. The read/write unit 13 is connected to a computer 15 (**green** below), which runs an “application program that is adapted to handle the flow of data coming in from the read/write unit 13.” *Id.*, 5:33-6:4. The computer 15 is connected to the Internet and transmits key information to remote servers including server 25 and data processing centre 26 (**red** below). *Id.*, 5:33-6:28.



Chies further discloses determining that a first device of a customer (e.g., a master transponder key such as original key 10) is communicating with a t/r device (e.g., read/write unit 13). Ex. 1004, 6:30-7:10 (describing, after a key 10 is introduced into read/write unit 13, using an “interactive read button 21” to “read[] the identification data of the key 10, thereby recognizing the type of key being handled” and optionally “the read/write unit 13 concurrently performs an inquiry operation to query the key 10” such that “a wireless communication is then established between the read/write unit 13 and the code-based electronic recognition means 11 of the key 10.”); Ex. 1002 ¶121.

To the extent this claim requires that the cloning application (e.g., Chies’ application program) performs this “determining” step, Chies discloses that its

application program does so when it receives the key information transmitted to it by read/write unit 13. Ex. 1004, 7:13-18 (“The read/write unit 13 transmits the INCODE, which contains also the information that identifies the key 10 to be duplicated in a univocal manner, owing to its having been assigned a log, to the computer connected thereto. The computer 15, as duly provided with the application program, receives such information and sends it to the serving computer or server 25.”). By successfully “receiving such information” (i.e., the INCODE data from the transponder key sent by read/write unit 13), the application program determines that the read/write unit 13 is communicating with a first device of a customer (e.g., key 10). Ex. 1002 ¶121.

If Patent Owner asserts that the “determining” step requires more than receiving data from the t/r device at the cloning application, then Marsh’s disclosure further underscores that this claim term is obvious under any construction of this claim term consistent with *Phillips*. Ex. 1002 ¶122. In particular, Marsh describes kiosk 200 automatically detecting the presence of a transponder key and establishing communication between the key and the transponder antenna 1302 within the kiosk. Ex. 1005, 22:38-44 (“[P]rocess 1800 can use transponder antenna 1302 and/or any other suitable device or combination of devices to automatically detect the presence of a transponder key (e.g., a transponder key inserted in slot 1404, a transponder key held near transponder

antenna 1302, etc.) using any suitable technique or combination of techniques.”).

Because Marsh’s kiosk 200 is a computing device running software (i.e., a cloning application) that reads information from a transponder key via transponder antenna 1302 and transmits that information to a remote server (*id.*, 17:51-18:9, 26:30-53), Marsh’s disclosure of its kiosk 200 automatically detecting the presence of the key and then reading information from that key is the manner of determining that the transponder key is communicating with transponder antenna 1302. Ex. 1002 ¶122.

A POSITA would have found it obvious to similarly implement automatic recognition in Chies’ system such that the application program of computer 15 automatically determines when a transponder key is inserted into read/write unit 13 and communication between the two devices is established, for example, to eliminate the need for a user to take additional steps to allow the application program to begin reading security information from the transponder key via read/write unit 13. Ex. 1002 ¶122. Doing so would have been well within the skill of a POSITA, and a POSITA would have had a reasonable expectation of success in doing so because it would require only routine and conventional computer programming techniques known in the art. Ex. 1002 ¶122; *see KSR*, 550 U.S. at 416-417, 421.

While Chies does not describe the shape of the antenna of read/write unit 13, a POSITA would have at least found it obvious to implement an antenna with a

ring shape into read/write unit 13 because such shapes were ubiquitous and well-known in the art, especially for devices reading information from transponders. Ex. 1002 ¶123. For example, as shown in annotated Figure 15 below, Marsh’s transponder antenna 1302 (**orange** below) within kiosk 200 is a ring-shaped “loop antenna” that reads security information from a transponder key. Ex. 1005, 16:23-58, Fig. 15; Ex. 1002 ¶123.

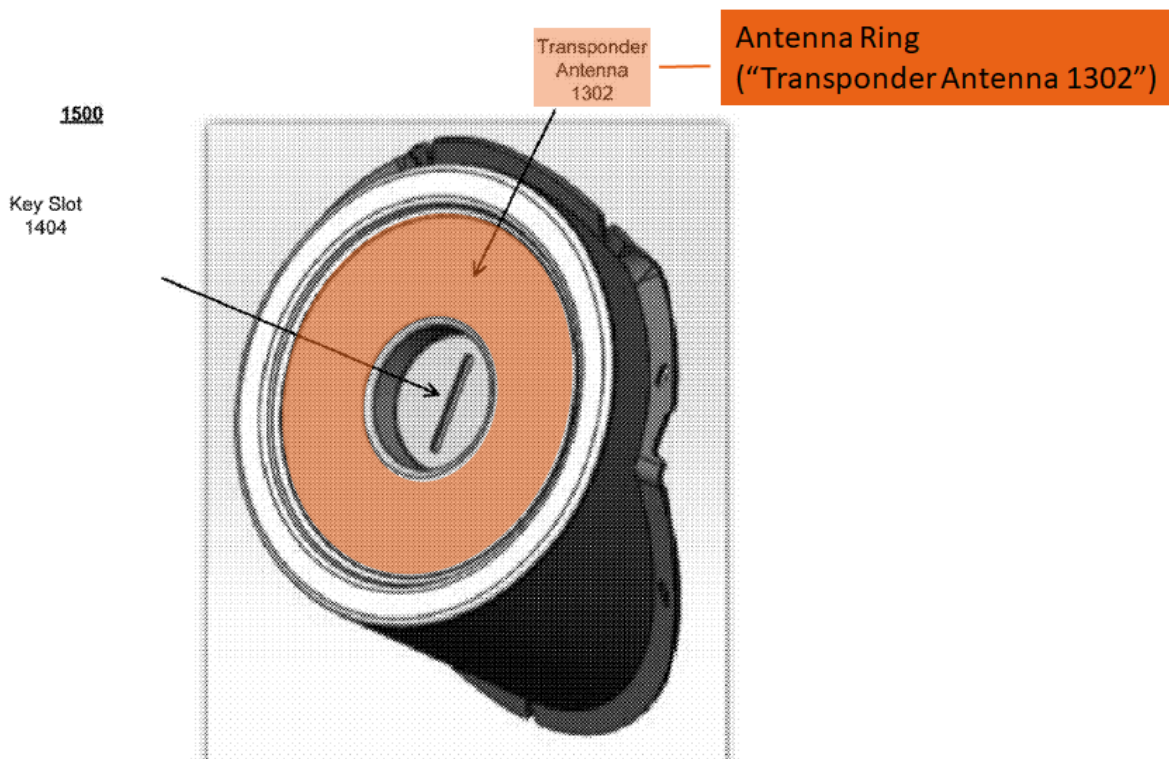


FIG. 15

Further demonstrating that such antennas were well-known in the art, Blalock discloses a ring-shaped antenna for reading information from a transponder key for a vehicle. Ex. 1006, 2:32-33 (describing “an antenna 215

which surrounds the slot 210” containing the transponder key), 3:21-37 (“The antenna 415 reads the transponder code off the transponder key 405”), Fig. 4; Ex. 1002 ¶124.

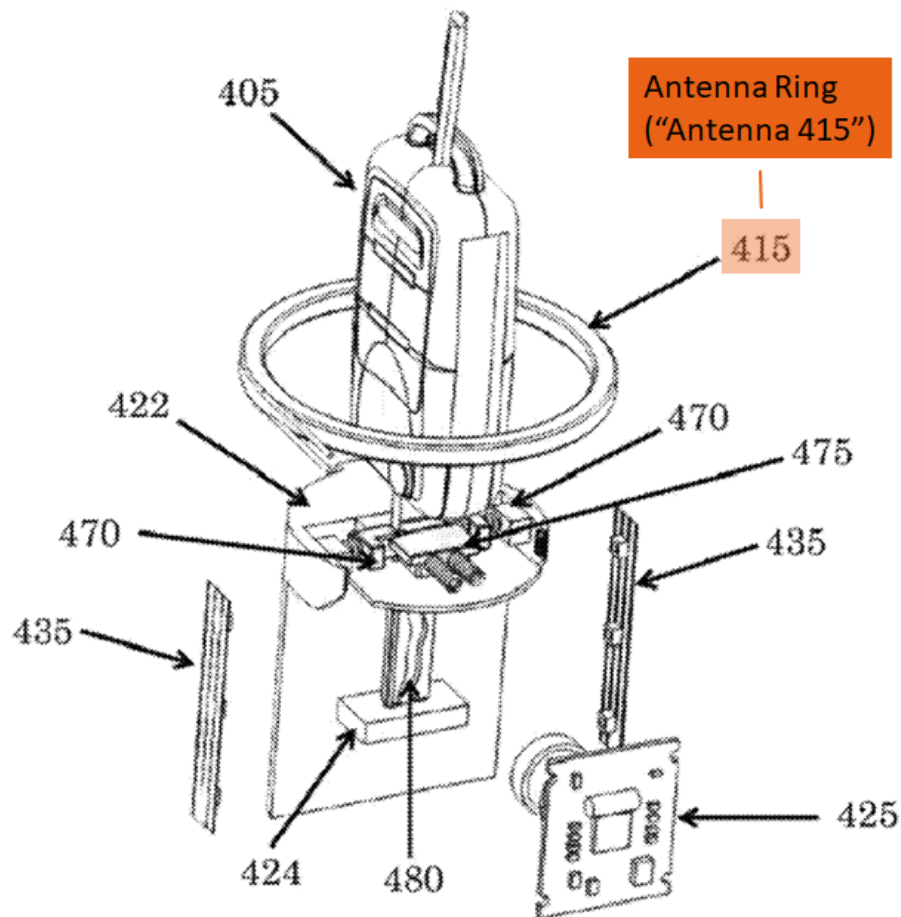


Figure 4

A POSITA would have implemented a ring antenna in Chies’ read/write unit 13 to fully surround the transponder key to more reliably read information from the transponder key, including by reading the transponder information regardless of the key’s spatial orientation (a known benefit of such antenna designs). Ex. 1002

¶125. In any event, implementing a ring antenna in Chies' read/write unit 13 would have been a matter of simple design choice well within the skill of a POSITA, especially in view of the known benefits of using a ring-shaped antenna. Ex. 1002 ¶125; *see KSR*, 550 U.S. at 417 (“[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.”), 421; *Uber*, 957 F.3d at 1338-41. A POSITA would have had a reasonable expectation of success for implementing a ring antenna into Chies' read/write unit 13 since such antennas are routinely used in the field for communicating with a transponder, and implementing such an antenna in Chies' read/write unit 13 would have required only routine skill and knowledge in the field. Ex. 1002 ¶125; *KSR*, 550 U.S. at 416-417, 421.

Chies alone, or in combination with Marsh, thus renders obvious determining that a first device of a customer is communicating with a t/r device, the t/r device including an antenna ring for wirelessly communicating with an access device for a vehicle. Ex. 1002 ¶¶120-126.

**6(c): retrieving security information digitally stored
by said access device;**

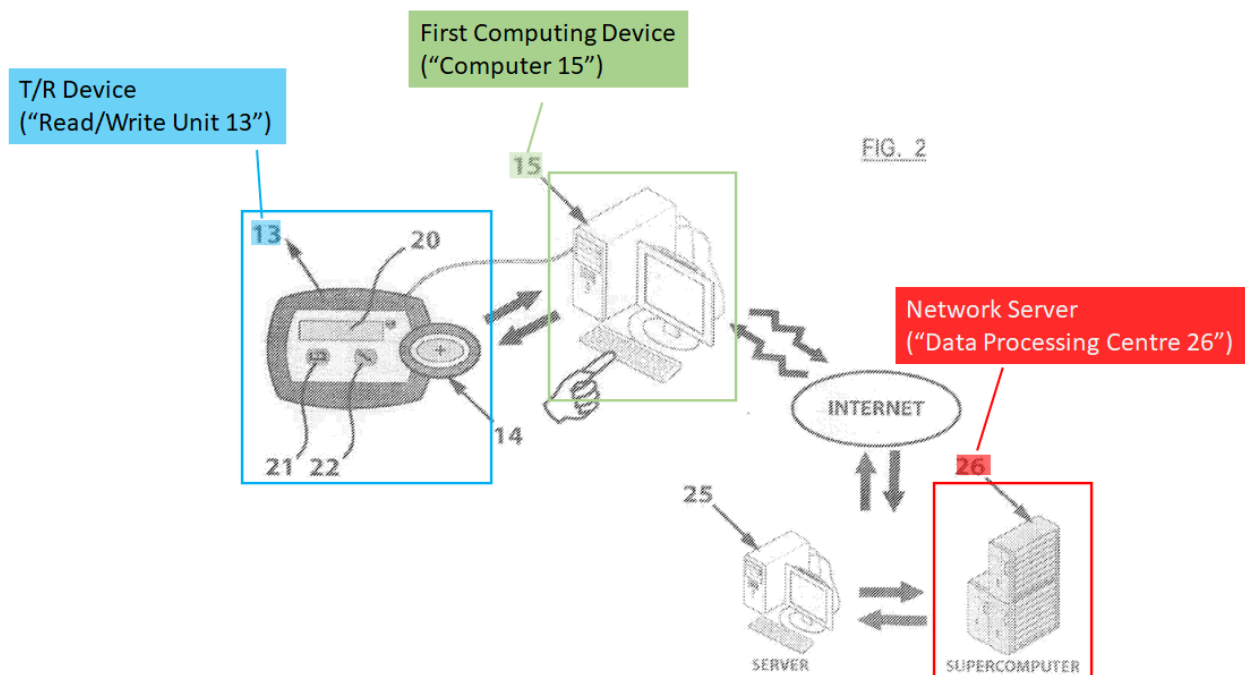
As discussed above, Chies discloses a t/r device (e.g., read/write unit 13) that includes an antenna for wirelessly communicating with an access device (e.g.,

original key 10). Ex. 1004, 4:31-5:2, 6:6-13 (“[T]he read/write unit 13 is provided with . . . an antenna (not shown) for receiving and transmitting data”), 7:4-5 (“[A] wireless communication is then established between the read/write unit 13 and the code-based electronic recognition means 11 of the key 10.”); Ex. 1002 ¶127. Chies further discloses retrieving security information digitally stored by the access device. Ex. 1004, 4:26-5:27 (describing storing security information in the memory of transponder key 10), 6:30-7:19 (“[A] key 10 to be duplicated is introduced in the appropriate receptacle 14 of a read/write unit 13. Via the interactive read button 21, the read/write unit 13 reads the identification data of the key 10, thereby recognizing the type of key being handled, and temporarily stores such data in the internal memory thereof.”); Ex. 1002 ¶127.

The information read from key 10 may be encrypted security information stored on the key. Ex. 1004, 6:30-7:10 (“In the assumption that the key 10 is of the type with a secret (encrypted) code, the read/write unit 13 concurrently performs an inquiry operation to query the key 10. Such query occurs through a code that is implemented in the read/write unit 13 and is solely known by the manufacturer.”). Chies refers to the security information received from the master key by read/write unit 13 as “INCODE.” Ex. 1004, 7:8-10 (“What the read/write unit 13 acquires is therefore a data-based information that is encrypted at random in a first encryption form, which shall be defined as INCODE hereinafter.”); Ex. 1002 ¶128.

6(d): communicating the security information for said access device to a network server;

Chies discloses communicating the security information (e.g., the INCODE data from read/write unit 13) for said access device (e.g., original key 10) to a network server (e.g., data processing centre 26). Ex. 1004, 6:15-7:31; Ex. 1002 ¶129. In particular, Chies discloses that read/write unit 13 transmits the INCODE data read from the original key to computer 15. Ex. 1004, 7:12-18 (The “computer 15, as duly provided with the application program, receives such information and sends it to the serving computer or server 25.”). Server 25 then transmits the INCODE data to data processing centre 26 (to which server 25 is connected over the Internet), where the INCODE data is processed. *Id.*, 6:15-28, 7:21-31, Fig. 2; Ex. 1002 ¶129.



Marsh similarly discloses receiving security information from a transponder key 1304 at kiosk 200 and transmitting that information over a communication link 1308 to a network server (e.g., server 1310) for processing the transponder information. Ex. 1005, 17:51-18:9 (“[K]iosk 200 can cause information received by transponder antenna 1302 to be transmitted to a server 1310 over a communication link 1308 and/or a communication network”), 19:10-24 (describing features of Marsh’s communication network 1606), 20:19-46 (same); Ex. 1002 ¶130. Server 1310 may be “a transponder key information server 1310 that facilitates identification of a proper transponder chip and/or transponder chip programming for a particular transponder key.” Ex. 1005, 20:36-46, Fig. 13.

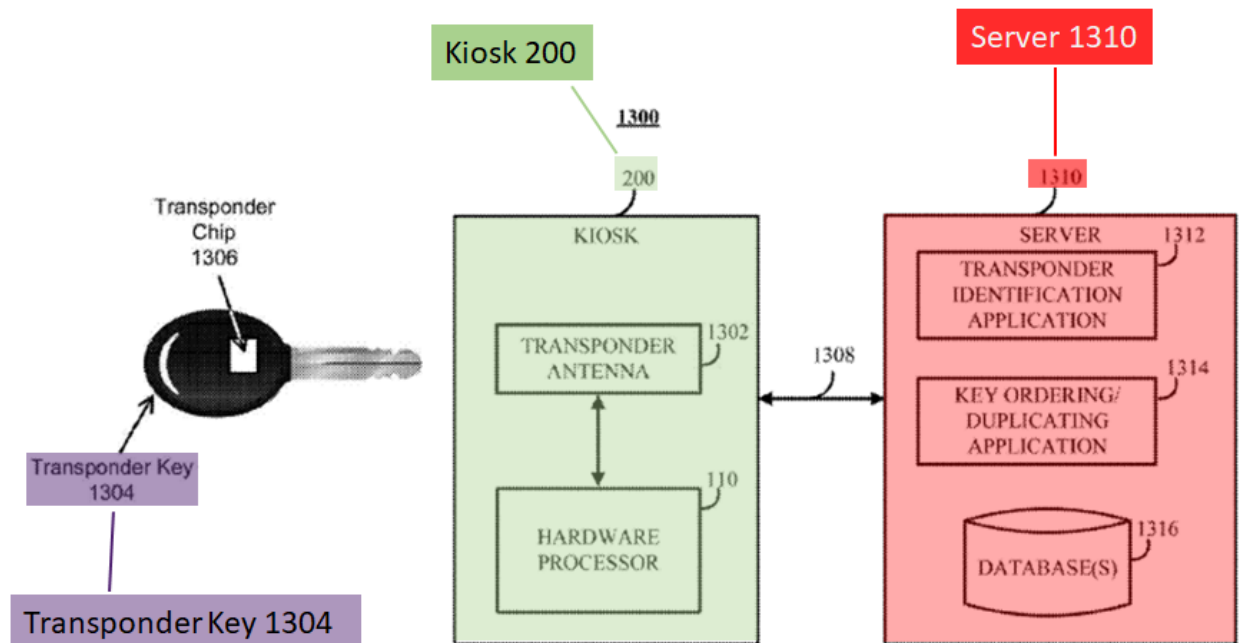


FIG. 13

6(e): generating a cloning security information; and

Chies discloses generating, by the network server (e.g., data processing centre 26), a cloning security information (e.g., “OUTCODE” data). Ex. 1004, 7:29-8:9. In particular, Chies describes processing the security information from the master key (e.g., the INCODE data) to prepare “OUTCODE” data used to program a blank transponder key. *Id.*, 7:29-8:9 (describing a process wherein “the INCODE is decrypted,” “the secret code is recognized and authenticated” such that “the single and sole secret code corresponding to the one contained in the microchip of the key 10 to be duplicated is acquired,” and “[t]he data processing centre 26 encrypts the corresponding secret code . . . into a second encryption form, which shall be defined as OUTCODE hereinafter.”), 8:21-34; Ex. 1002 ¶131.

As discussed above for Claim 2, it would also have been obvious to generate a cloning security information using the cloning application (e.g., the application program of Chies’ computer 15) in view of the disclosures of Chies and Marsh. Ex. 1002 ¶¶76-89. Chies in combination with Marsh thus renders obvious generating a cloning security information. Ex. 1002 ¶¶131-132.

6(f): transmitting the cloning security information to the t/r device to program a duplicate access device with the cloning security information; and

Chies discloses transmitting the cloning security information (e.g., “OUTCODE” data) to the t/r device (e.g., read/write unit 13) to program a

duplicate access device (e.g., blank key 30) with the cloning security information. Ex. 1004, 8:11-34; Ex. 1002 ¶133. After receiving the OUTCODE data, read/write unit 13 “transfers all identification data of [original key 10] into the microchip of the new blank key 30, wherein this operation is performed with the aid of the interactive write button 22.” Ex. 1004, 8:21-29. The OUTCODE data is then “decrypted and definitively stored – along with the other identification data – solely inside the microchip of the blank key 30.” *Id.*, 8:29-31. The blank key 30 is then “able to exactly emulate the functions of the configuration of the original key.” *Id.*, 8:31-34.

6(g): a processor configured to execute the instructions.

As discussed above for Claim 6(a), Chies discloses the use of a computer 15 that includes the application program that reads key information from the master transponder key via the read/write unit 13. Ex. 1004, 5:33-6:28 (“Installed in the same computer 15 there is an application program that is adapted to handle the flow of data coming in from the read/write unit 13.”), 7:12-19 (“The read/write unit 13 transmits the INCODE . . . to the computer connected thereto. The computer 15, as duly provided with the application program, receives such information and sends it to the serving computer or server 25.”); Ex. 1002 ¶¶116-119. While Chies does not expressly describe a processor within computer 15, a

POSITA would have understood that computer 15 would include a processor that executes instructions associated with the application program. Ex. 1002 ¶134. Such processors are ubiquitous in computers and have been used for decades, and a POSITA would have interpreted Chies' computer 15 as including such a processor. Ex. 1002 ¶134.

To the extent that Chies lacks express details regarding a processor in computer 15, the use of such a processor would have been obvious in view of Marsh. Ex. 1002 ¶135. Marsh discloses a processor configured to execute instructions stored on a non-transitory computer-readable storage medium, such as the computer processor within kiosk 200. Ex. 1005, 19:54-20:18 (kiosks 200 “can include any of a general purpose device such as a computer,” which may include “any suitable components such as a hardware processor” and “memory”), 20:47-62 (describing “a non-transitory computer-readable medium . . . for storing a computer program for controlling hardware processor 1702,” wherein “[h]ardware processor 1702 can use the computer program to execute the mechanisms described herein for duplicating keys and/or duplicating transponder keys and managing the key information thereof”), 24:34-61 (kiosk 200 is a “computing device executing process 1800” for duplicating a transponder key), 26:30-53 (describing the use of a computer program “that causes a processor (such as hardware processor 110, hardware processor 1702 and/or hardware processor

1722) to execute the mechanisms described herein,” such as a computer program “written in a programming language recognizable by kiosk 200”).

To the extent it would have been necessary to modify Chies’ computer 15 to include a processor to execute the instructions stored on a non-transitory computer-readable storage medium such as Marsh’s, a POSITA would have been motivated to do so to allow computer 15 to execute the instructions, thus allowing Chies’ application program to function, and would have had a reasonable likelihood of success in doing so given that the use of such processors is routine and well-known in the field. Ex. 1002 ¶136; *see KSR*, 550 U.S. at 416-417, 421.

Chies alone, or in combination with Marsh, thus renders obvious a processor configured to execute instructions. Ex. 1002 ¶¶134-137.

VII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION TO DENY INSTITUTION

A. The Board Should Not Deny Institution Under § 325(d)

The Board should not exercise its discretion to deny institution. The relevant considerations are: (1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and (2) if either condition of first part of the framework is satisfied, whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims.

Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH, IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020).

Neither factor warrants denial of institution. During prosecution, the Examiner found the claims patentable in view of the claimed “t/r device including an antenna ring for wirelessly communicating with an access device for a vehicle,” as well as “retrieving security information digitally stored by said access device.” Ex. 1003, 157 (emphasis in original). But as explained in Section VI, Chies and/or Marsh discloses the features that the Examiner failed to find in the prior art, and neither Chies nor Marsh was submitted to the Office during prosecution or considered by the Examiner. As a result, the Examiner did not consider the same (or substantially the same) combination of prior art and arguments during prosecution that are presented in this Petition, and the Examiner’s failure to consider references such as Chies and Marsh moreover constitutes an error material to the patentability of the challenged claims.

B. The Board Should Not Deny Institution Under § 314(a)

The ’455 patent has not been asserted in litigation, nor have any related patent family members. The Board should therefore not exercise its discretion to deny institution under § 314(a).

VIII. GROUNDS FOR STANDING

Petitioner certifies that the '455 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting *inter partes* review challenging the patent claims on the grounds identified herein.

IX. MANDATORY NOTICES

A. Real Party-in-Interest

The real party-in-interest is The Hillman Group, Inc.

B. Related Matters

Petitioner is not aware of any related matters.

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Lead Counsel	Back-Up Counsel
Joshua L. Goldberg (Reg. No. 59,369) joshua.goldberg@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue, NW Washington, DC 20001 Tel: 202-408-4000 Fax: 202-408-4400	Ryan P. O'Quinn (Reg. No. 67,191) oquinnr@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 1875 Explorer St. Suite 800 Reston, VA 20190 Tel: 571-203-2700 Fax: 202-408-4400 Daniel F. Klodowski (Reg. No. 72,693) daniel.klodowski@finnegan.com Finnegan, Henderson, Farabow, Garrett & Dunner, LLP 901 New York Avenue, NW Washington, DC 20001 Tel: 202-408-4000 Fax: 202-408-4400

D. Service Information Under 37 C.F.R. § 42.8(b)(4)

Please address all correspondence to counsel at the addresses above.

Petitioner consents to service by email at the above addresses.

X. CONCLUSION

The Board should institute IPR and cancel the claims. The Office may charge any required fees to Deposit Account No. 06-0916.

Respectfully submitted,

Dated: November 2, 2022

/Joshua L. Goldberg/
Joshua L. Goldberg (Reg. No. 59,369)
Lead Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(a)(1)(i), the undersigned hereby certifies that the foregoing PETITION FOR *INTER PARTES* REVIEW contains 12,808 words, excluding parts of this Petition exempted under § 42.24(a), as measured by the word-processing system used to prepare this paper.

Dated: November 2, 2022

/Joshua L. Goldberg/

Joshua L. Goldberg (Reg. No. 59,369)
Lead Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing **Petition for *Inter Partes* Review**, the associated **Power of Attorney**, and **Exhibits 1001 through 1007** are being served on November 2, 2022, by FedEx Priority Overnight® at the following address of record for the subject patent.

Mark Masterson
McDonald Hopkins LLC
600 Superior Avenue, East
Suite 2100
Cleveland, OH 44114

/Lisa C. Hines/
Lisa C. Hines
Senior Litigation Legal Assistant
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP