REMARKS

Favorable reconsideration, reexamination, and allowance of the present patent application are respectfully requested in view of the foregoing amendments and the following remarks.

I. Examination Under Pre-AIA First to Invent Provisions

The present application is being examined under the *pre-AIA* first to invent provisions.

II. Request for Continued Examination (RCE)

This Amendment is submitted conjunction with the Request for Continued Examination ("RCE") under 37 C.F.R. § 1.114(d). An Amendment Under 37 C.F.R. § 1.116 was filed on November 2, 2020 (November Amendment), but not entered. An Advisory Action was mailed on August 12, 2020.

III. Advisory Action

The Advisory Action indicates that the Examiner has considered the amendments and arguments submitted with the November Amendment. However, the Advisory Action asserts that Applicant's November Amendment fails to place the present application in condition for allowance. The present Amendment is a modification of the November Amendment that addresses the additional comments of the Advisory Action.

IV. The Examiner Interviews

Applicant appreciates the courtesies extended to Applicant's representative by Examiner Henning in the December 17, 2020 and December 22, 2020 Interviews. As reflected in the Interview Summaries, various aspects of the invention, the applied art and various proposed changes to the claims were discussed.

In response to the discussions in the Interview, Applicant has variously amended the claims. In particular, the claims are amended as discussed and agreed upon to overcome the current rejection under pre-AIA 35 U.S.C. 103(a) to more clearly recite that the authentication

data previously claimed refers to a private key used to generate a signature. The claims are also amended to further satisfy 35 U.S.C. 112 and for clarity. For at least the reasons set forth herein, Applicant submits that the claims define patentable subject matter. Reconsideration is respectfully requested.

V. Allowable Subject Matter

Applicant gratefully acknowledges the indication, at page 16 of the Office Action, that claims 11, 15, and 16 include allowable subject matter.

VI. Summary of the Office Action

The Office Action rejects claims 23-25 under 35 U.S.C. 112(b) or *pre-AIA* 35 U.S.C. 112 as being indefinite.

The Office Action rejects claims 1-10, 12-14, and 21-28 under *pre-AIA* U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No.: 2003/0041250 to Proudler ("Proudler") and further in view of U.S. Patent Publication No.: 2002/0095557 to Constable, *et al.* ("Constable") and U.S. Patent Publication No.: 2002/0099666 to Dryer ("Dryer").

The Office Action rejects claims 17-20 under *pre-AIA* U.S.C. § 103(a) as being unpatentable over Proudler and Constable and further in view of WIPO Publication No.: WO/2000/067143 to Unicate ("Unicate").

The Office Action provisionally rejects claims 1-28 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-2, 4, 7-8, 10-11, 13-25, 29, 33-38, and 42-43 of co-pending U.S. Patent Application No. 10/560,579.

VII. Summary of Response to Office Action

In response to the September 18, 2020 Final Office Action, claims 1, 2, 5-15, 21, 22 and 26-28 are amended, claims 3, 4, 16, 17, 18, 19, 20, 23, 24, and 25 are cancelled without prejudice or disclaimer, and new claim 29 is added. Accordingly, claims 1, 2, 5-15, 21, 22, and 26-29 are currently pending, of which claims 1, and 26-28 are the only pending independent claims.

Specifically, independent claims 1, and 26-28 are amended to include the features of claim 16 and replace authentication data with a private key. Support for this amendment is found in previous claims defining authentication data for generating a digital signature and mention of private keys in para. [0106]. Claims 3, 4, and 17-20 are cancelled without prejudice or disclaimer. Claims 23, 24, and 25 are also cancelled to comply with requirements of form under 35 U.S.C. § 112 in response to the objections set forth in the Final Office Action. New claim 29 is based at least on previous claim 25, support for which can also be found at least on page 12, lines 31-37 of the specification as originally filed of the present application.

Applicant respectfully submits that the amendments to the claims made herewith are consistent with the specification as originally filed. No new matter is included with the changes to the claims in the present Amendment.

VIII. 35 U.S.C. § 103(a)

The Office Action rejects claims 1-10, 12-14, and 21-28 under *pre-AIA* U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No.: 2003/0041250 to Proudler ("Proudler") and further in view of U.S. Patent Publication No.: 2002/0095557 to Constable, *et al.* ("Constable") and U.S. Patent Publication No.: 2002/0099666 to Dryer ("Dryer"); and claims 17-20 under *pre-AIA* U.S.C. § 103(a) as being unpatentable over Proudler and Constable and further in view of WIPO Publication No.: WO/2000/067143 to Unicate ("Unicate"). Applicant respectfully traverses these rejections and requests reconsideration for the following reasons.

At the outset, Applicant gratefully acknowledges the indication from Examiner Henning that the presented Amendments will overcome the current rejection. Applicant respectfully submits that independent claims 1 and 26-28 are amended to include the feature of "wherein the private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software."

None of the applied art, including Proudler, Constable, Dryer, and Unicate, teach at least this feature. Accordingly, and as further discussed below, none of the prior art nor the art

applied in the Office Action, either alone or in combination, teach or suggest attaining the advantages provided by this feature recited in in each of the independent claims.

Specifically, Proudler, Constable, Dryer, and Unicate are entirely silent with respect to an encrypted private key. As a result, none of Proudler, Constable, Dryer, or Unicate, either alone or in combination, can disclose a decryption key for decrypting the private key. Accordingly, any proposed combination of the prior art fails to disclose at least the feature of "wherein the **private key is decrypted in a secure processing environment inaccessible to said user and to any user-operated software**," as recited in each of independent claims 1, 26, 27, and 28, emphasis added.

The advantages of this feature include improved protection both of the private key (authentication data) that is used by an electronic device to generate digital signatures, and of a decryption key for decrypting the private key, which decryption key is incorporated in the electronic device. The private key is encrypted when stored in a secure location in the electronic device. However, the private key still needs to be used in unencrypted form to generate digital signatures. To this end, a decryption key is incorporated in the electronic device, which can be used to decrypt the private key. The decryption is a particularly sensitive processing step, since it involves two particularly sensitive pieces of data: the private key which, when intercepted, could be used to forge signatures; and the decryption key which, when intercepted, could be used to undo the encryption of the private key. The decryption operation is particularly sensitive since it uses these two pieces of information *in combination* and thus an attack on the decryption operation would be particularly impactful.

Interestingly, however, the inventors envisaged to perform the decryption in a secure processing environment, which is inaccessible to the user, any user-operated software, and to the operating system. This way, it is prevented that the user can access the private key and decryption key at the time when they are both being processed together as part of the decryption of the private key. It is also prevented that user-operated software can access this particularly sensitive processing step. Thus, through the use of a secure processing environment, access to the decryption key and the private key during the decryption is denied for example to malware

inadvertently installed by the user, but also to software deliberately installed or operated by the user in an attempt to access the decryption key and/or private key.

Accordingly, protection is improved against internal attacks, *e.g.*, attacks originating in the device's own operating system or from the device's own user. At the priority date, it was a new insight that preventing internal attacks is important; the features in the independent claims provides a novel and inventive way to address that concern.

The applied art does not disclose nor teach or suggest this feature and are thus not able to attain the specific advantages in terms of protection against internal attacks that this feature provides. Accordingly, at least due to the inclusion of this feature, the independent claims 1, 26, 27, and 28 are distinguishable over the applied art. As previously argued, Applicant maintains that the present claims include other features that that are distinguishable over the applied art, and thus, the claims not obvious and patentable for at least these previously argued reasons as well.

In the present case, as described above, neither of the cited references either alone or in combination teaches or suggests all features of Applicant's claims. Thus, the Office Action immediately fails to establish a *prima facie* case of obviousness as to these claims.

Because none of the prior art of record nor any of the applied art, either alone or in combination, teach the above-referenced features, as well as other features, of Applicant's claims 1, 26, 27, and 28, it is respectfully submitted that there is no *prime facie* case for obviousness. Therefore, Applicant respectfully requests that the rejection of independent claims 1, 26, 27, and 28 under *pre-AIA* U.S.C. § 103(a) be withdrawn. Further, Unicate fails to make-up for the above deficiencies. Thus, the dependent claims are similarly distinguishable over the applied art at least for the above reasons for which independent claims 1, 26, 27, and 28 are not obvious, and for the separate features that each of these claims recites. Applicant respectfully requests that the rejection of the dependent claims under *pre-AIA* U.S.C. § 103(a) be withdrawn.

IX. Double Patenting

The Office Action provisionally rejects claims 1-28 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-2, 4, 7-8, 10-11, 13-25, 29, 33-38, and 42-43 of co-pending U.S. Patent Application No. 10/560,579. Applicant respectfully traverses this rejection and requests reconsideration for the following reasons

A provisional rejection based on nonstatutory double patenting was raised in the Office Action. However, the claims are patentably distinct from each other. The difference regarding a private key being decrypted in a secure processing environment inaccessible to a user and to any user-operated software, has been shown above not to be obvious. The Applicant maintains that other differences regarding the encryption of the private key and the secure storage of the decryption key are non-obvious as well. Since copending application No. 10/560,579 has not yet been granted, it is requested this rejection be kept in abeyance until copending application No. 10/560,579 is allowed.

X. Conclusion

Applicant respectfully submits that the present patent application is in condition for allowance. An early indication of the allowability of this patent application is therefore respectfully solicited.

If the patent examiner believes that a telephone conference with the undersigned would expedite passage of this patent application to issue, they are invited to call on the number below.

It is not believed that extensions of time are required, beyond those that may otherwise be provided for in accompanying documents. If, however, additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a), and the Commissioner is hereby authorized to charge fees

necessitated by this paper, and to credit all refunds and overpayments, to our Deposit Account listed herein.

Respectfully submitted,
KENEALY VAIDYA LLP

By: /Eric D. Morehouse/
Eric D. Morehouse
Registration No. 38,565

Erik N. Lund
Registration No. 77,473

U.S.P.T.O. Customer Number 39083
KENEALY VAIDYA LLP
3050 K Street, NW Suite 302
Washington, DC 20007
202.748.5913 (direct)
202.748.5902 (main)
Deposit Account 50-6840

Date: December 23, 2020