



- (51) **International Patent Classification:** Not classified
- (21) **International Application Number:** PCT/IB2014/001207
- (22) **International Filing Date:** 14 March 2014 (14.03.2014)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:** 61/791,612 15 March 2013 (15.03.2013) US
- (71) **Applicant:** ASSA ABLOY AB [—/SE]; Klarabergs-
viadukten 90, S-111 64 Stockholm (SE).
- (72) **Inventor:** WELLER, Gunther; Grethenstrasse 8, 35398
Giessen (DE).
- (74) **Agents:** MUIRHEAD, Donald, W. et al.; Muirhead And
Saturnelli, Llc, 200 Friberg Parkway, Suite 1001, Westbor-
ough, MA 01581 (US).
- (81) **Designated States** (*unless otherwise indicated, for every
kind of national protection available*): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,

BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.

- (84) **Designated States** (*unless otherwise indicated, for every
kind of regional protection available*): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

- *without international search report and to be republished
upon receipt of that report (Rule 48.2(g))*



WO 2014/140922 A2

(54) **Title:** SECURE KEY DISTRIBUTION FOR MULTI-APPLICATION TOKENS

(57) **Abstract:** Provisioning a token includes providing at least one key to a secure key vault, determining an available slot on the token, transferring the at least one key to a key load SAM, and transferring at least one of: the at least one key and/or other applica-
tion data from the key load SAM to the available slot on the token. A token issuer may use the key load SAM to load the at least one
key onto the token. A service provider may provide the at least one key to the secure key vault. The at least one key may allow an
end user to use the token to access a service provided by the service provider. The token may be a cell phone or a smart card. The se-
cure key vault may be implemented using cloud storage.

SECURE KEY DISTRIBUTION FOR MULTI-APPLICATION TOKENS

TECHNICAL FIELD

This application is related to the field of digital credential management and, more particularly, to the field of digital credential management using multiple entities.

BACKGROUND OF THE INVENTION

Multiple applications may reside in a security token, such as a smart card. A centralized management arrangement may be installed inside the security token or provided externally to the security token to load key(s) and/or data into the token to facilitate the different applications. The centralized management arrangement may be controlled by the security token issuer (manufacturer) and may provide complete control over all applications in the security token.

While advantageous in many commercial deployments, an issuer-centric model does not necessarily fit deployments where unaffiliated application providers desire to configure and maintain key(s) and/or application data associated with each application. For security reasons, some application providers may not wish to give the token issuer or other unaffiliated applications access to key(s) and/or application data for an application.

It is desirable to provide a system that addresses shortcomings of token issuing systems described above.

SUMMARY OF THE INVENTION

According to the system described herein, provisioning a token includes providing at least one key to a secure key vault, determining an available slot on the token, transferring the at least one key to a key load SAM, and transferring the at least one key and/or other application data from the key load SAM to the available slot on the token. A token issuer may use the key load SAM to load the at least one key onto the token. The token issuer may not access the at least one key. The at least one key may be provided in an encrypted form that cannot be decrypted by the token issuer. A service provider may provide the at least one key to the secure key vault. The at least one key may allow an end user to use the token to access a service provided by the service provider. Each of the slots may store keys and other application data from different service providers. The token may be a cell phone or a smart card. Prior to transferring the at least one key from the key load SAM to the available slot on the token, the key may be digitally signed and/or encrypted. The secure key vault may be implemented using

cloud storage. A service provider may use the² key load SAM to load the at least one key and/or the other application data onto the token. A plurality of secure key vaults may communicate with the key load SAM. The plurality of secure key vaults may coordinate free slots available on the token.

According further to the system described herein, computer software, provided in a non-transitory computer-readable medium, provisions a token. The software includes executable code that provides at least one key to a secure key vault, executable code that determines an available slot on the token, executable code that transfers the at least one key to a key load SAM, and executable code that transfers the at least one key and/or other application data from the key load SAM to the available slot on the token. A token issuer may use the key load SAM to load the at least one key onto the token. The token issuer may not access the at least one key. The at least one key may be provided in an encrypted form that cannot be decrypted by the token issuer. Each of the slots may store keys and other application data from different service providers. The token may be a cell phone or a smart card. The secure key vault may be implemented using cloud storage.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the system described herein are explained with reference to the several figures of the drawings, which are briefly described as follows.

FIG. 1 is a schematic illustration showing a secure key vault, a token issuer, a key load SAM, and a plurality of service providers according to an embodiment of the system described herein.

FIG 2 is a schematic illustration showing a token with slots according to an embodiment of the system described herein.

FIG. 3 is a flow diagram showing processing in connection with loading key(s) and/or application data into a token by a token issuer according to an embodiment of the system described herein.

FIG. 4 is a schematic illustration showing a secure key vault, a token issuer, a key load SAM, and a service provider according to an embodiment of the system described herein.

FIG. 5 is a flow diagram showing processing in connection with loading key(s) and/or application data into a token by a service provider according to an embodiment of the system described herein.

FIG. 6 is a schematic illustration showing a plurality of secure key vaults, a token issuer, and a key load SAM according to an embodiment of the system described herein.

DETAILED DESCRIPTION OF VARIOUS EMBODIMENTS

Referring to FIG. 1, a diagram 100 illustrates a system for managing customer keys and/or other application data that is stored on a token, such as a smart card. The system includes a secure key vault 102, and a token issuer 104 (token manufacturer) that securely communicates with the secure key vault 102. The system 100 also includes a plurality of independent (unaffiliated) service providers 106-108 that are in secure communication with the secure key vault 102. Although FIG. 1 shows three service providers, there may be any number of service providers. The independent service providers 106-108 facilitate various secure services (applications) of possible interest to a user of the token, such as banking, building access, access to television/movie services such as the Netflix service, etc.

Each of the secure services requires that one or more secret keys and/or other application data are loaded onto the token. The secret keys may be symmetric key(s) used in connection with communication between the service providers 106-108 and the token after the token has been deployed. The other application data may be data that is used in connection with accessing a service provided in connection with the token and corresponding with a specific application (e.g., an account number for bank service). The system 100 provides a mechanism where the service providers can have the secret keys and/or application data loaded onto the tokens without necessarily having a direct relationship with the token issuer 104 and without the token issuer 104 having any access to the key(s) and/or application data. As explained in more detail herein, the service providers 106-108 have a relationship with the secure key vault 102 and it is the secure key vault 102 that has a relationship with the token issuer 104. In addition, the key(s) and/or application data are loaded into the token in a secure way that prevents the token issuer 104 from accessing the key(s) and/or application data, except possibly in encrypted form. That is, the token issuer 104 may send and/or receive the key(s) and/or application data in an encrypted form that cannot be decrypted by the token issuer 104.

The token issuer 104 uses a key load SAM 112⁴ to facilitate the secure transfer of keys and/or application data from the secure key vault 102 to tokens issued by the issuer 104. The key load SAM 112 may be implemented as a tamper-proof smartcard that contains one or more keys that provide encryption and authentication in communications between the secure key vault 102 and the tokens issued by the token issuer 104. The key load SAM 112 may include software on a crypto module. In an embodiment herein, both the secure key vault 102 and the token issued by the token issuer 104 use a PKI public/private key pair for encryption and authentication (digital signing). Of course, other appropriate cryptographic and authentication mechanisms may be used instead, provided that communication between the secure key vault 102 and the token is secure and the source of data can be authenticated (i.e., via digital signing).

FIG. 1 shows that the issuer 104 delivers a token to an end user 114. The token received by the end user includes one or more secure key(s) and/or application data for one or more services from the service providers 106-108. The application data may be used for obtaining specific service(s) from the service providers 106-108. Note that the secure keys and/or application data may be provided on the token without the end user having any direct relationship with the service providers 106-108 and without the issuer 104 having any direct relationship with the service providers 106-108. Thus, the system described herein reduces the number of entities to which the service providers 106-108 need to establish and maintain a secure relationship. In an embodiment herein, the service providers 106-108 establish a secure relationship only with the secure key vault 102 and perhaps other secure key vaults (not shown in FIG. 1). In some embodiments, the key load SAM 112 encrypts and/or digitally signs key(s) and/or application data stored on the token by the key load SAM 112.

Referring to FIG. 2, a token 122 is shown in detail as including a plurality of slots 124-126. Each of the slots 124-126 represents secure memory space of the token 122, which can be used to store secure key(s) and/or application data for one of the service providers 106-108. Although FIG. 2 shows three slots, there may be any number of slots in the token 122. In an embodiment herein, each of slots 124-126 is either empty or holds secure key(s) and/or application data for only one of the service providers 106-108. Of course, in other embodiments, it is possible for one of the slots 124-126 to contain key(s) and/or application data for more than one service provider. As discussed elsewhere herein the key(s) and/or application data may be encrypted.

The secure key vault 102 assigns and ⁵keeps track of which of the slots 124-126 contain secure key(s) and/or application data for each of the service providers 106-108. Thus, for example, the secure key vault 102 may assign the slot 124 to the service provider 106, the slot 125 to the service provider 107, etc. In some embodiments, any key(s) and/or application data in a slot for a particular one of the service providers 106-108 may be further encrypted to provide access to only the particular one of the service providers 106-108, to the exclusion of other ones of the service providers 106-108. Also note that, in some embodiments, the keys are symmetric so that a secret shared key on the token is identical to a secret shared key used by a corresponding service provider. In such a case, it may be advantageous to encrypt the symmetric key to prevent other applications and the token issuer 104 from accessing the symmetric key. That is, the token issuer does not receive a clear text version of the key and cannot decrypt an encrypted version of the key.

Referring to FIG. 3, a flow diagram 140 illustrates operation of the system 100 in connection with the issuer 104 providing key(s) and/or application data to a token on behalf of one of the service providers 106-108. Processing begins at a first test step 142 where it is determined if the particular token being provisioned is authorized for the particular service for which key(s) and/or application data are being obtained. In some embodiments, only some of the service providers 106-108 provide service for only some of the tokens issued by the issuer 104. For example, only some of the end users may be obtaining television-related services, in which case token(s) corresponding to end user(s) not receiving the service would be determined to be not authorized at the step 142. If it determined at the step 142 that a particular token is not authorized for a particular service being provisioned, then control transfers from the test step 142 to a step 144 where error processing is performed. The error processing performed at the step 144 can include providing a message to a user/operator that the requested provisioning cannot be performed. Following the step 144, processing is complete. In some embodiments, error processing performed at the step 144 may simply exit the provisioning program.

If it is determined at the test step 142 that the token being provisioned is authorized for one or more requested service(s), then control transfers from the test step 142 to a step 146 where a secure connection is established between the secure key vault 102 and the key load SAM 112 at the token issuer 104. Following the step 146 is a step 148 where a currently empty slot on the token is selected for provisioning with the key(s) and possibly other data of the service provider. Following the step 148 is a step 152 where the key(s) and possibly other data for the service provider are transferred from the secure key vault 102 to the key load SAM 112.

Following the step 152 is a step 154 where the⁶ key load SAM is used to load the key(s) and/or application data onto the token. As discussed elsewhere herein, in some embodiments, the key load SAM 112 encrypts and/or digitally signs key(s) and/or application data stored on the token by the key load SAM 112. Following the step 154, processing is complete. Note that, in an embodiment herein, the key(s) may be provisioned onto the token in a way that prevents both unrelated service providers and even the token issuer from ascertaining the key(s). Thus, in the case of shared secret key(s) that are shared between the token and a corresponding service provider, for example, the system described herein reduces the likelihood of the key(s) being compromised.

Referring to FIG. 4, a diagram 160 illustrates an embodiment where the end user 114 presents a previously-issued token to the service provider 106 to add key(s) and/or application data to the token to add the service provided by the service provider 106. In the embodiment illustrated in FIG. 4, the end user 114 is adding a service that was not previously provided on the token. For example, the end user 114 may be adding access to a particular building that the end user 114 did not access at the time the token was issued.

The secure key vault 102 communicates with a key load SAM 162 of the service provider 106. The key load SAM 162 of the service provider 106 is similar to the key load SAM 112 of the issuer 104. In the embodiment of FIG. 4, the service provider 106 provides provisioning in a manner similar to the provisioning provided by the issuer 104, discussed above. However, in the embodiment of FIG. 4, there is no issuer (since the token was previously issued); instead, a service is being added to the already-issued token.

Referring to FIG. 5, a flow diagram 170 illustrates steps performed in connection with provisioning a token according to the embodiment illustrated in FIG. 4, discussed above. Processing begins at a first step 172 where a secure connection is established between the secure key vault 102 and the key load SAM 162 of the service provider 106. Following the step 172 is a test step 174 where it is determined if a slot is available on the token. Note that it is possible for an end user to inadvertently attempt to add a new service to a token having all available slots already used. If it is determined at the test step 174 that there are no slots available, then control transfers from the test step 174 to a step 176 where error processing is performed. The error processing performed at the step 176 can include providing a message to the end user indicating that there is no room on the user's token to provision a new service. Following the step 176, processing is complete.

If it is determined at the test step 174⁷ that the token being provisioned does have an available slot, then control transfers from the test step 174 to a step 178 where a currently empty slot on the token is selected for provisioning with the key(s) and/or application data of the service provider. Following the step 178 is a step 182 where the key(s) and possibly other application data are transferred from the secure key vault 102 to the key load SAM 162. Following the step 182 is a step 184 where the key load SAM 162 is used to load the key(s) and/or application data onto the token. As discussed elsewhere herein, in some embodiments, the key load SAM 162 encrypts and/or digitally signs key(s) and possibly other application data stored on the token by the key load SAM 162. Following the step 184, processing is complete. Note that, just as with the embodiment of FIG. 1, discussed above, the key(s) may be provisioned onto the token in a way that prevents any unrelated service providers from ascertaining the key(s). Thus, for example, in the case of shared secret key(s) that are shared between the token and the service provider, the system described herein reduces the likelihood of the key(s) being compromised.

Referring to FIG. 6, a diagram 190 illustrates a system with a plurality of secure key vaults 192-194. Although FIG. 6 shows three secure key vaults, there may be any number of secure key vaults. The secure key vaults 192-194 may be interconnected (not shown in FIG. 6) to communicate and coordinate free slots for tokens serviced and provisioned by the secure key vaults 192-194. Each of the secure key vaults 192-194 may be connected with one or more service providers (not shown in FIG. 6) in a manner similar to the secure key vault 102 connected to the service providers 106-108, described above. Note that two or more of the secure key vaults 192-194 may be connected to the same service provider to provide fault tolerance. It is also possible for each of the secure key vaults 192-194 to be connected to different service providers. Each of the secure key vaults 192-194 communicates with token issuer 196 having a key load SAM 198 similar to the key load SAM 112 discussed above.

The system described herein includes a token that is provisioned to work with a service provider. The token may be a cell phone or a portion thereof. For example, a cell phone may be provisioned to provide physical access for a user. The token (e.g., cell phone) may communicate using a network and may use a LAN, WAN, Bluetooth, Wi-fi, etc. Some or all data and/or key(s) used in connection with one or more of the services may be provided and/or maintained using cloud storage. The secure key vault may be implemented using cloud storage.

The system described herein may be used with any mechanism for provisioning a token to provide service(s) to a holder of the token. Various embodiments discussed herein may be combined with each other in appropriate combinations in connection with the system described herein. Additionally, in some instances, the order of steps in the flowcharts or flow diagrams may be modified, where appropriate. Further, various aspects of the system described herein may be implemented using software, hardware, a combination of software and hardware and/or other computer-implemented modules or devices having the described features and performing the described functions. Software implementations of the system described herein may include executable code that is stored in a computer readable storage medium and executed by one or more processors. The computer readable storage medium may include a computer hard drive, ROM, RAM, flash memory, portable computer storage media such as a CD-ROM, a DVD-ROM, a flash drive and/or other drive with, for example, a universal serial bus (USB) interface, and/or any other appropriate tangible storage medium or computer memory on which executable code may be stored and executed by a processor. The system described herein may be used in connection with any appropriate operating system.

Other embodiments of the invention will be apparent to those skilled in the art from a consideration of the specification or practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only.

What is claimed is:

1. A method of provisioning a token, comprising:
 - providing at least one key to a secure key vault;
 - determining an available slot on the token;
 - transferring the at least one key to a key load SAM; and
 - transferring at least one of: the at least one key and other application data from the key load SAM to the available slot on the token.
2. A method, according to claim 1, wherein a token issuer uses the key load SAM to load the at least one key onto the token.
3. A method, according to claim 2, wherein the token issuer does not access the at least one key.
4. A method, according to claim 3, wherein the at least one key is provided in an encrypted form that cannot be decrypted by the token issuer.
5. A method, according to claim 1, wherein a service provider provides the at least one key to the secure key vault.
6. A method, according to claim 5, wherein the at least one key allows an end user to use the token to access a service provided by the service provider.
7. A method, according to claim 1, wherein each of the slots stores keys and other application data from different service providers.
8. A method, according to claim 1, wherein the token is one of: a cell phone and a smart card.
9. A method, according to claim 1, wherein prior to transferring the at least one key from the key load SAM to the available slot on the token, the application data is at least one of: digitally signed and encrypted.
10. A method, according to claim 1, wherein the secure key vault is implemented using cloud storage.

11. A method, according to claim 1, wherein a service provider uses the key load SAM to load at least one of: the at least one key and the other application data onto the token.
12. A method, according to claim 1, wherein a plurality of secure key vaults communicate with the key load SAM.
13. A method, according to claim 12, wherein the plurality of secure key vaults coordinate free slots available on the token.
14. Computer software, provided in a non-transitory computer-readable medium, that provisions a token, the software comprising:
 - executable code that provides at least one key to a secure key vault;
 - executable code that determines an available slot on the token;
 - executable code that transfers the at least one key to a key load SAM; and
 - executable code that transfers at least one of: the at least one key and other application data from the key load SAM to the available slot on the token.
15. Computer software, according to claim 14, wherein a token issuer uses the key load SAM to load the at least one key onto the token.
16. Computer software, according to claim 15, wherein the token issuer does not access the at least one key.
17. Computer software, according to claim 16, wherein the at least one key is provided in an encrypted form that cannot be decrypted by the token issuer.
18. Computer software, according to claim 14, wherein each of the slots stores keys and other application data from different service providers.
19. Computer software, according to claim 14, wherein the token is one of: a cell phone and a smart card.
20. Computer software, according to claim 14, wherein the secure key vault is implemented using cloud storage.

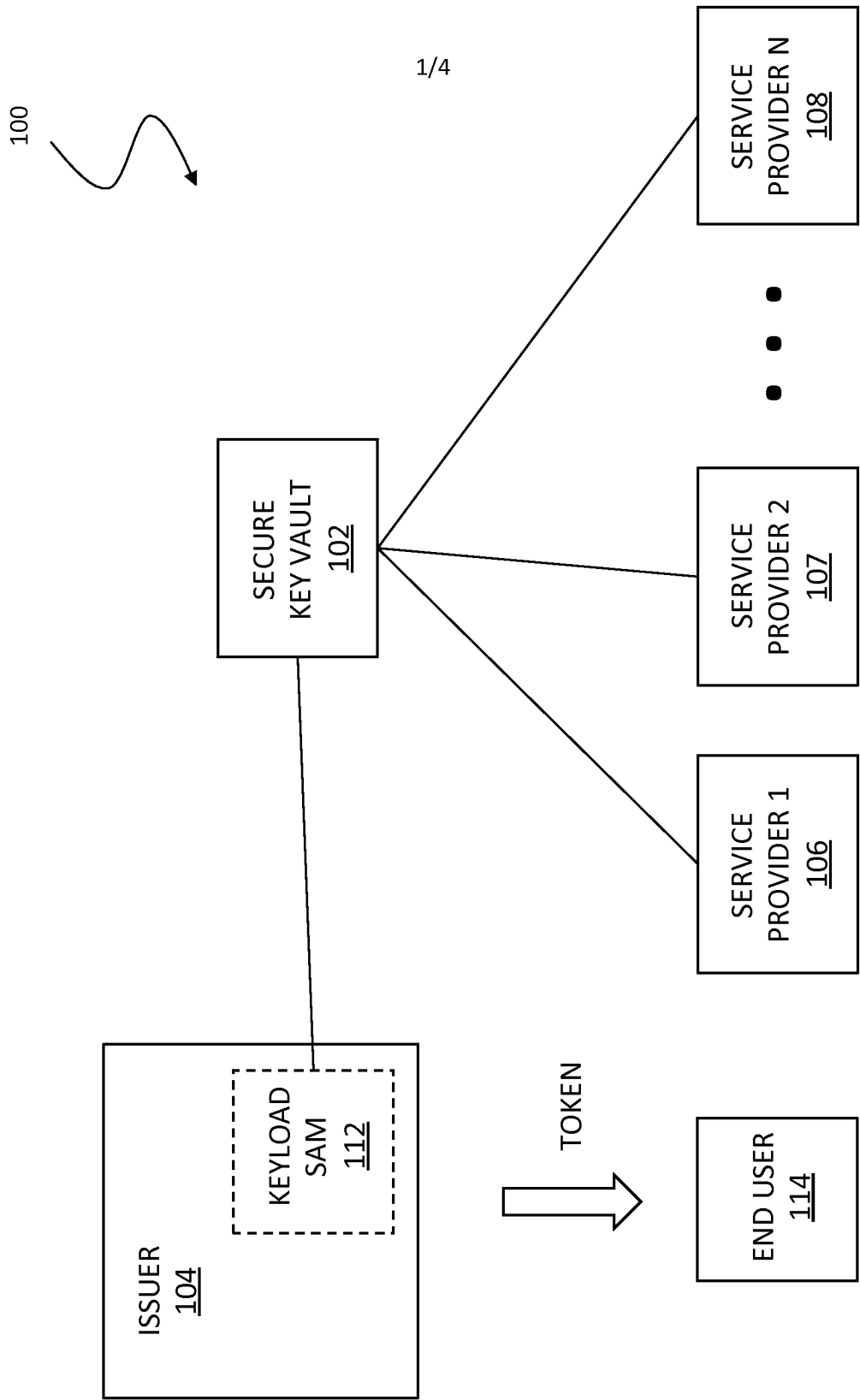


FIG. 1

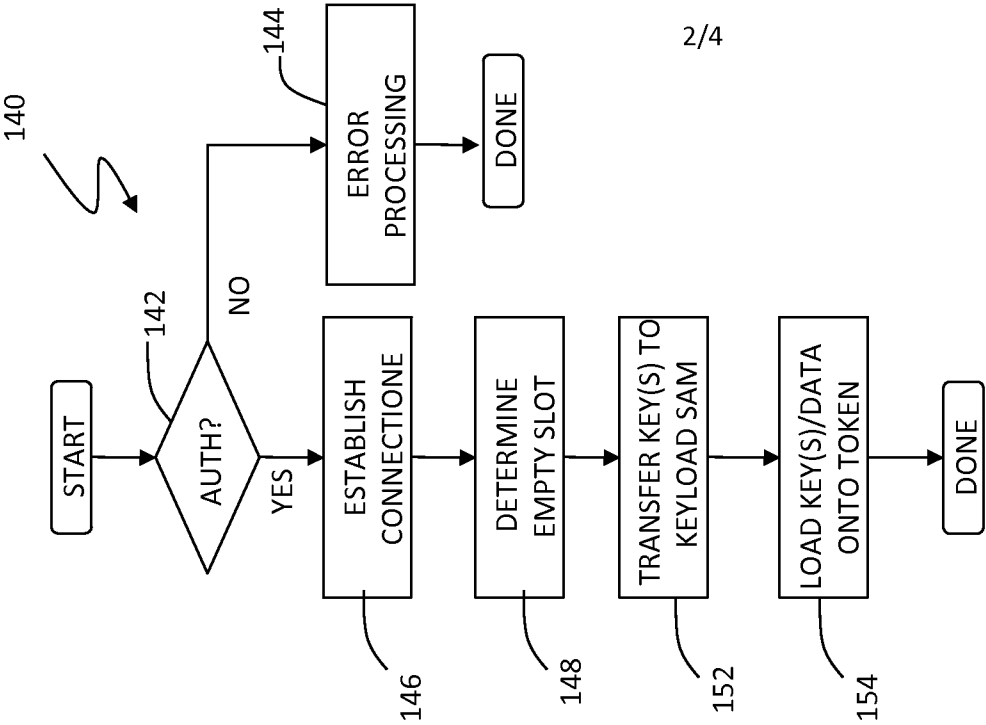


FIG. 3

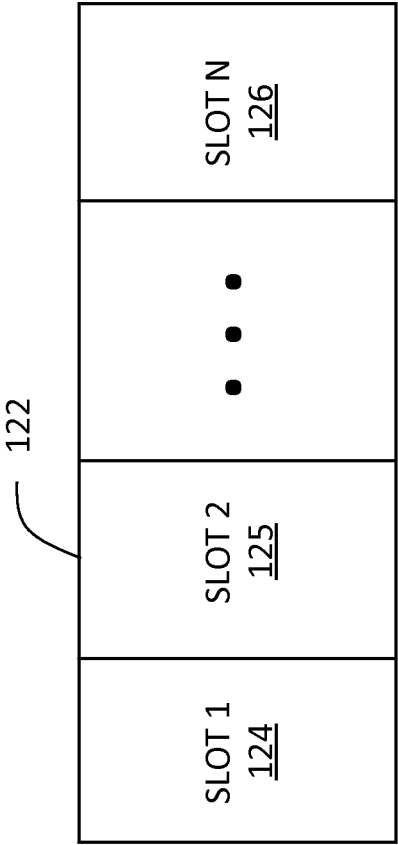


FIG. 2

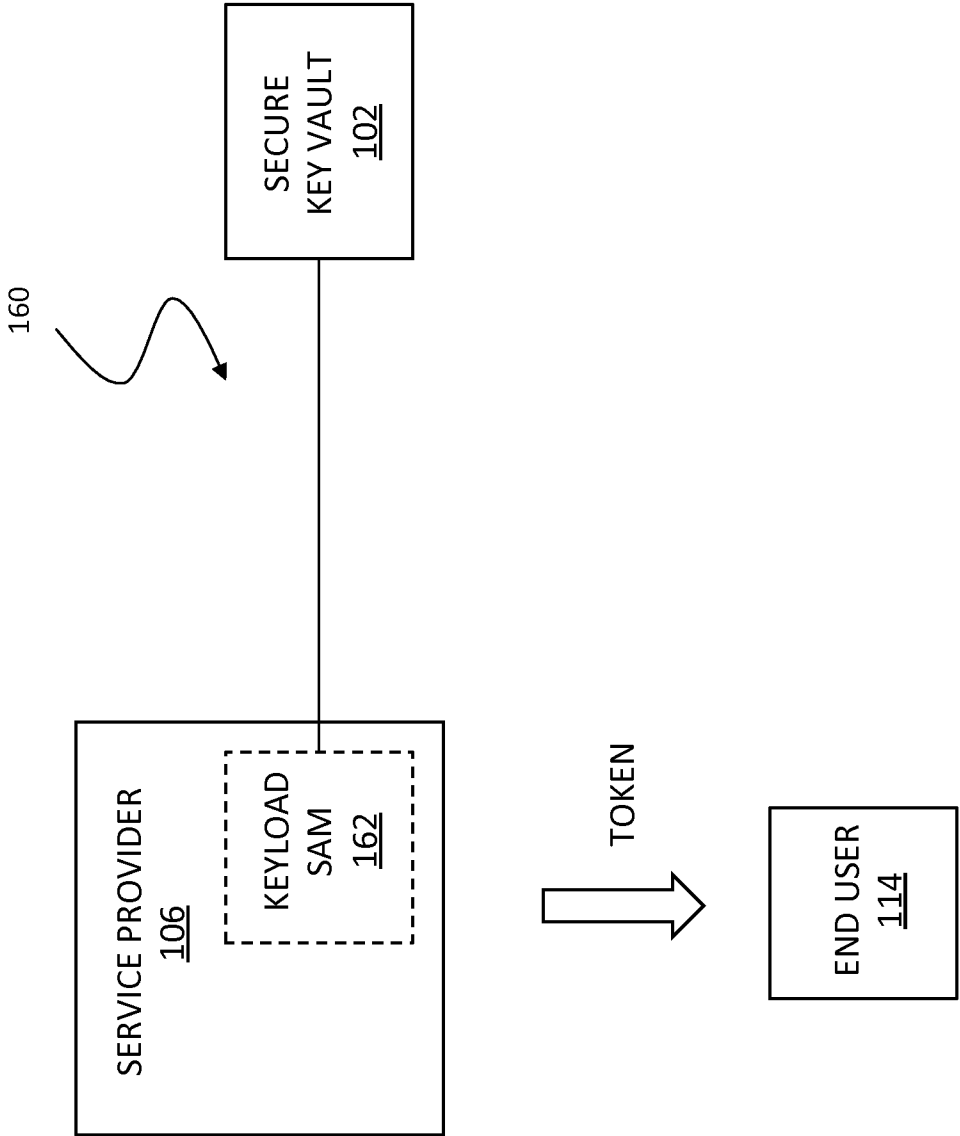


FIG. 4

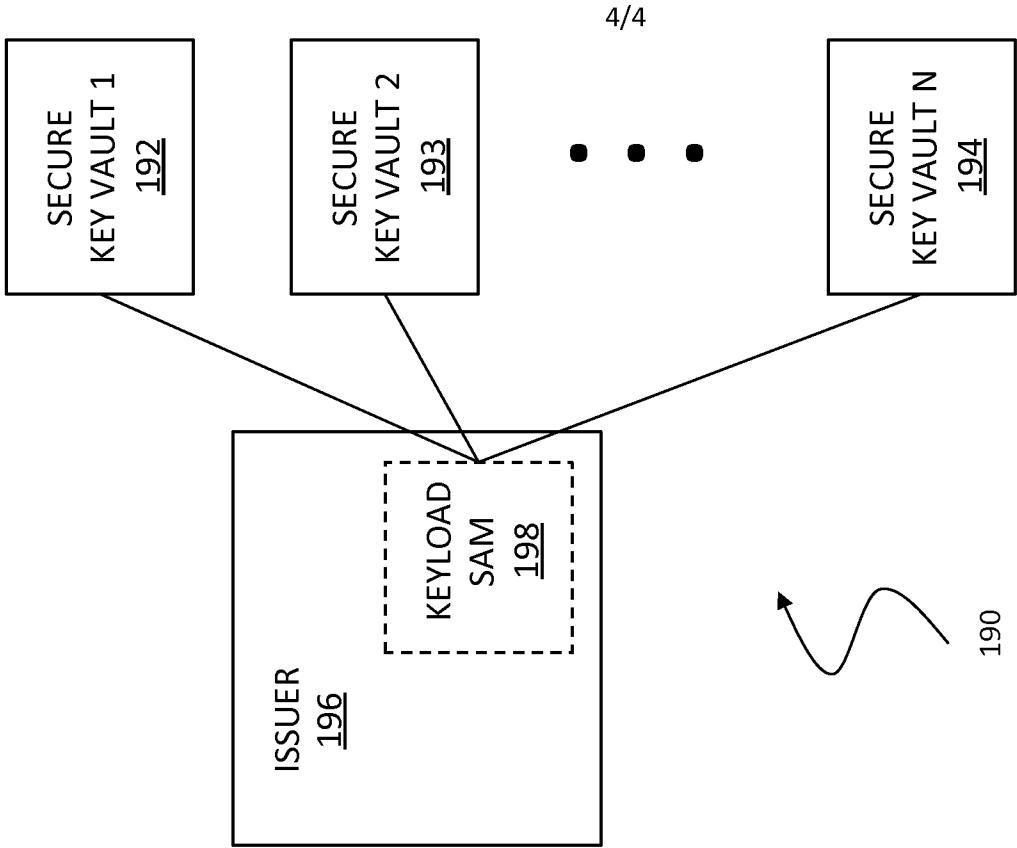


FIG. 6

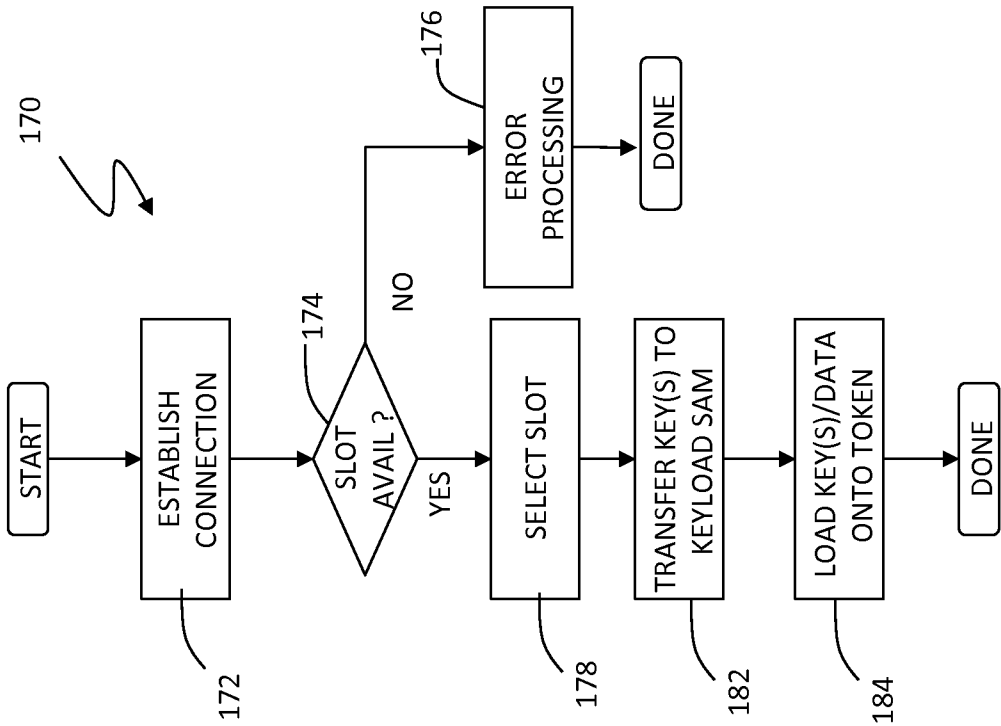


FIG. 5