



SENSITIVE DATA NEEDS MORE THAN PASSWORD PROTECTION



CONTENTS

1

SecSign ID	3
1.1 SecSign ID Authentication Overview	3
1.2 Technical Facts	5
1.2.1 Key Generation and Registration	5
1.2.2 Authentication Schematic	8
1.2.3. Patented SafeKey-Procedure: Defense Against Brute Force Attacks Against the Key	12
1.2.4. Key Change	12
1.2.5 Restoring a SecSign ID after Loss of a Mobile Device	13
1.2.6 Locking and Disabling an ID	13
1.2.7 Using the SecSign ID on Several Devices	14
1.3 Protective Measures of the Infrastructure	14
1.3.1. SecSign ID Server: Data Management and Reliability	14
1.3.2. Firewall and SecSign Routing Server Protection of the SecSign ID Server	14
1.3.3 The SecSign ID Server is NOT a Web Server	15
1.3.4 Integration for any Web Portal, Application, or Service	15
1.4. Product Differences Compared to Other Solutions:	15
1.4.1. Data Minimization (No Phone Numbers, SMS, etc.)	15
1.4.2 The Role of PIN / Password	16
1.5 Unique Features of SecSign ID Two-factor Authentication	16
1.5.1 Security of the Authentication Procedure	16
1.5.2. Single Sign-on	16
1.6 ID Server as On-premise Solution	17
1.7. Additional Advantages Compared to Common Authentication Solutions	18
1.8. SecSign ID Similarity to Authentication with Smart Cards	18

2

SecSign Portal	19
2.1. Data Security	19
2.1.2. Six-eyes Principle	19
2.1.3 Protection of the Portal Server	19
2.1.3.1 Web Application Firewall	20
2.1.3.2. Encryption in Detail (AES 256-bit Encryption)	20

SecSign ID offers unique and highly secure two-factor authentication for any web portal, application, or service. Though SecSign ID is engineered with advanced cryptography, the registration, login, and authentication procedures are simple and require minimal time and effort by the user.

The level security is similar to that of a login with a smart card. But SecSign ID offers greater convenience, accessibility, and cost-effectiveness than card-based solutions because there is no need for special card reader hardware.

SecSign ID provides out-of-band, mobile two-factor authentication based on public key infrastructure (PKI). The applied challenge-response procedure is based on an algorithm that generates asymmetric key pairs up to a length of 2048 bits each. Each 2048-bit key contains 617 decimal digits, and their asymmetry poses enormous practical difficulty in factoring the product of these two large prime numbers. In fact, this cryptography is impossible to defeat with any current or anticipated integer factorization or computing power, including quantum computing.



In this section, you will find an overview of the authentication process, technical facts about SecSign ID, details about protection of the authentication infrastructure, and additional information about unique features, benefits, and advantages of SecSign ID.

For more information, please visit: www.secsign.com

1.1 SECSIGN ID AUTHENTICATION OVERVIEW

SecSign ID enables users to verify their digital identity and authenticate access to services by using their smartphone or tablet device. The required steps for identity verification and user authentication are explained below.

The SecSign ID approach to two-factor authentication eliminates all of the security vulnerabilities and usability issues that plague other authentication methods, providing unsurpassed user access protection by removing passwords and replacing them with cryptography procedures that make it physically impossible to compromise logins via hacking, phishing, and malware. This protection also includes total security against man-in-the-middle attacks, SIM card cloning, and phone number porting schemes that have been used to bypass SMS two-factor authentication.

Importantly, this superior approach avoids the entry or transmission of passwords or any other sensitive credentials during the login process, meaning that it is physically impossible for attackers to steal user credentials. No confidential credentials are ever entered, transmitted, or stored for the purposes of logins. Instead, SecSign ID uses mobile push authentication and public key infrastructure (PKI), which relies on the same fundamental security principles and the same combination of knowledge and possession that is used in smart card security.

SecSign ID Mobile Push PKI Authentication Involves Three Core Elements:

1. A 2048-bit encrypted private key is encoded and secured on the user's mobile device. The private key is secured by a patented SafeKey mechanism that prevents brute force attacks, even if a user's mobile device is lost or stolen.
2. A 2048-bit public key is stored and secured on a Trust Center server, which can be deployed in the cloud or by configuring and operating your own authentication server, with the same security on your own architecture.
3. Physical possession and rightful ownership of the private key is confirmed through one of several verification options, which allow the private key to digitally sign an authentication challenge that is generated by the authentication server via an encrypted channel.

With this approach, the login process provides the best possible security and simplifies authentication by eliminating the use of passwords and sensitive credentials. The login and authentication process is simple and can be completed within seconds using a login on any website or application, with authentication completed using a simple mobile app.

As usual, users log into the secured service through a website or application, but the user enters only a non-confidential user ID and does not enter a password. The user ID is non-confidential because there is no need to secure it: the ID cannot be used on its own to access the account or obtain any confidential information.

Once the user ID is entered, the web or app server communicates with the authentication server, which issues a challenge that must be digitally signed by the private key on the user's mobile device. The mobile app is used to digitally sign the challenge with the 2048-bit encrypted private key.

Four Options Available to Verify User Identity on the mobile device

To confirm possession of the encrypted private key on the user's mobile device, and allow it to digitally sign the authentication request, the user must verify identity through knowledge and/or biometrics. SecSign ID offers four ways to do this (depending on the user's device):

1. Enter a user-defined PIN or a passcode (which is used only in the app and never transmitted). The PIN or passcode is not used in authentication and is merely used to verify and protect physical access to the ID on the mobile app.
2. Use fingerprint biometrics, such as Apple's Touch ID, to confirm private key ownership
3. Combine a user-defined PIN or passcode with a fingerprint. This creates a combination of knowledge and biometrics for extra security.
4. Use only the physical presence of the private key on the mobile device to verify authentication. While this option removes the PIN, passcode, or fingerprint protection for the private key, it still provides a stronger alternative to password-based logins because the private key exists only on the user's mobile device, so only someone who possesses the device can access the user's account.

An Access Symbol Provides Final Confirmation

Once ownership of the private key is confirmed, the mobile app shows a set of four symbols. The user taps the symbol that matches one shown on the login screen of the secured website or application, and this provides final identity verification. The mobile app notifies the authentication server of the result, and access to the user account is granted.

SecSign ID Makes It Impossible for Attackers to Steal User Credentials

Using mobile push PKI authentication, a user can complete authentication in just a few seconds, and all of this happens without using a password and without entering, transmitting, or storing any sensitive credentials as part of the login process. This means that there is physically nothing for criminals to steal or use to gain unauthorized access to accounts or data. No amount of brute force hacking, phishing, malware, man-in-the-middle attacks, or SIM card attacks will provide them with a credential that can be used to authenticate access to a user account.

Thus, it is possible to implement a level of security that is even stronger than the two-factor authentication used by most major banks to protect online banking logins, but this can be done by using a method that is actually simpler and easier for users.

1.2 TECHNICAL FACTS

1.2.1 Key Generation and Registration

Introduction

The key pair for SecSign ID authentication is generated on the user's mobile device. For this, the SecSign app generates an asymmetric key pair. A public key is transmitted with TLS encryption to the server and then deleted on the mobile device. The asymmetric private key is encrypted (AES/SafeKey) with the PIN or passcode and stored on the mobile device. **Neither the passcode nor the associated private key are ever transmitted and can therefore not be intercepted by an attacker.**

For authentication, the user needs the private key which is encrypted and then stored with further AES encryption on the mobile device. The key is protected against brute force attacks against the private key and against the AES encryption by the use of the SafeKey method. The SafeKey mechanism is explained in section 1.2.3 below: **SafeKey Procedure.**

If the user generates an ID, it will be immediately registered on the associated ID server. The user can then immediately use the ID for authentication.

The SecSign ID app enables the user to generate new key pairs at any time for an existing ID. For this, the key on the smartphone, as well as the key of the ID server, is replaced.



Key Pair Generation

The SecSign app locally creates an asymmetric key. The key length (currently 2048 bits) is defined in the SecSign app by the manufacturer. The user enters a desired user name for the SecSign ID, which will be accepted as long as that ID is available and has not yet been assigned on the SecSign ID server.

The SecSign ID server is by default id1.secsign.com (a public server operated through Amazon Web Services by SecSign Technologies).

A SecSign ID can be configured on a different ID server by using a specific menu option and entering the address of the other server. Using this option allows customers to configure IDs to connect to an on-premise server that they can operate on their own architecture, behind their firewall, e.g. with a turnkey virtual appliance licensed and supplied by SecSign Technologies.

For more information about deploying an on-premise SecSign ID server, please see section 1.6 of this document: ***SecSign ID Server as an On-premise Solution.***

Access Protection

To provide physical access protection for the private key, the user can enter a PIN or passcode. This is used to verify user identity during authentication, and it is also used in the SafeKey encryption of the private key.

If a fingerprint scan is used instead of a PIN or passcode, and if a fingerprint is stored on the device, this fingerprint will be defined as an access condition for the generated private key.

Though we do not recommend it, SecSign ID can also be configured so that a PIN, passcode, or fingerprint is not used for access protection. Thus, the user will not be required to enter a PIN or passcode or scan a fingerprint during authentication. Only the physical presence of the encrypted private key will be used to verify identity. This approach is still much more secure than other authentication methods because it still requires a true, physical authentication factor in the form of the private key. And authentication takes place out-of-band and never requires the entry of a password, one-time code, or other sensitive credential through the login mechanism.

However, we recommend that a PIN, passcode, or fingerprint be used for stronger protection. So, by default, SecSign ID prompts the user to define a PIN or passcode or scan a fingerprint in order to protect access to the user's SecSign ID.

SafeKey Encryption of the Private Key

If a PIN or passcode is entered into the app when creating the SecSign ID, the private key is encrypted with the PIN or passcode. If no PIN or passcode exists (e.g. the fingerprint was selected for access protection), 16 random bytes will be used for encryption and stored in the device's key chain. With the algorithm PBKDF2, an AES key encryption key is derived from the PIN, passcode, or random bytes. If the user does not use any access protection like PIN, Touch ID or passcode, a random password (coming from the key chain) will still be used for encryption. The private key will therefore never be unprotected.

The private key is used as an indication for the encryption in a format which cannot be differentiated from random data. A modulus and private exponent are connected with each other and encrypted with AES in cipher block chaining mode by using the key encryption key.

Thus, even if an attacker could somehow access the encrypted key and, by trying out all possible 4-digit PINs, receive the correct key, the attacker will not be able to notice this success. The public key is only on the SecSign ID server and not in the SecSign app. In order to check that the private key is correctly decrypted, the attacker must authenticate against the server. The server, however, counts unsuccessful attempts and will lock the key after 10 unsuccessful attempts.

This is why a 4-digit PIN provides sufficient protection for the private key. And this procedure has been patented in the U.S. under the name SafeKey.

The user's private key, which is protected by the SafeKey method, is stored in the mobile device's key chain. Also, for added protection: In case the user backs up a mobile device in iTunes, the private key will only be included in the backup, if the the backup is encrypted.



Registration

After its generation in the SecSign app, the public key is protected by TLS-encryption and sent to the SecSign ID server in order to register the SecSign ID under the user's chosen user name. For this, the SecSign ID server verifies that the user name has a configurable minimum length and does not originate from a defined set of reserved definitions. The server also verifies that the SecSign ID app has transmitted a signature which is suitable for the public key (i.e. the app actually contains the encrypted private key).

Priority Code

Afterwards, the server generates a priority code for the SecSign ID. This is to protect the user in case of an attempted denial-of-service attack in which an attacker continuously generates login sessions in an attempt to block the user from authenticating. The SecSign ID server only allows one login at a time, so such an attack might otherwise trigger this restriction. However, if such an attack ever occurs, the priority code will be shown to the authorized user in the SecSign app. The priority code indicates to the server or administrator which login session is being generated from the rightful, authorized user, and thus allows the server to grant access.

Storage of the SecSign ID

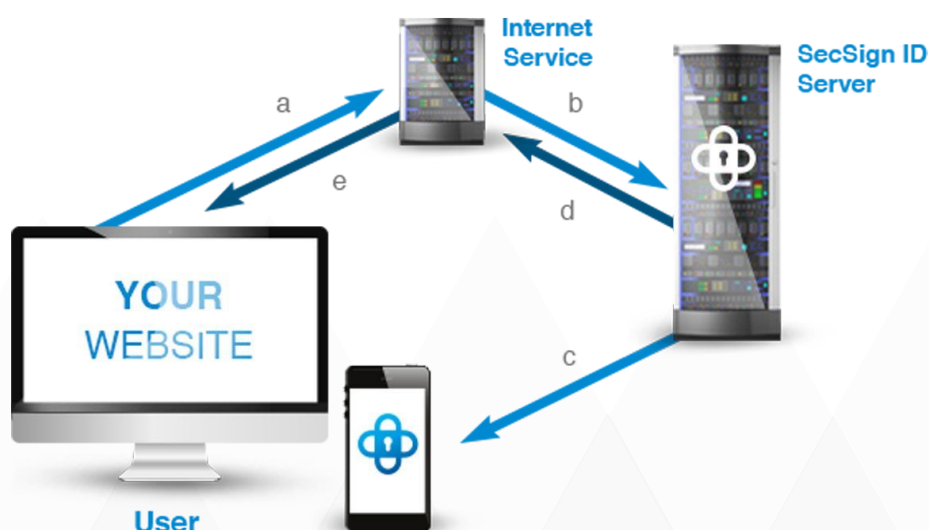
The SecSign ID server stores the new SecSign ID in the SQL database (Oracle, Microsoft SQL server, DB/2, MySQL, PostgreSQL, Sybase, etc.) and transmits the data to a redundant fallback SecSign ID server where the data is also stored. Both servers are running in parallel and, if possible, in different geographic regions and enable the user to log in, even if one of the servers is not available. The two public SecSign ID servers of SecSign Technologies are located on the east and on the west coast of the United States. Finally, the administrator receives an email notification of the newly generated SecSign ID.

1.2.2 Authentication Schematic

The login on a website, application, or other service secured by SecSign ID is realized through a challenge-response procedure. Authentication is only possible if the user has the required mobile device that contains the encrypted private key (physical factor) and knows the PIN or passcode of the associated ID (knowledge factor) or can provide the required fingerprint scan (biometric factor). This ensures that a minimum of two distinct authentication factors are always required in order to authenticate. Optionally, three-factor authentication can be enabled by requiring all three factors, or access protection can be removed so that only the physical presence of the private key on the mobile device is used for identity verification and authentication.

The process of the authentication is shown in the following diagram:

- 1 The user enters a user name (SecSign ID) into a web browser. The associated web portal or service invokes an access symbol from the SecSign ID server for this user name.



The diagram shows what the web server will request from the identity server (SecSign ID server).

What Happens During This Step:

- a) User enters the SecSign ID through the Internet service
- b) Internet service requests authentication from the ID server
- c) ID server sends push notification to the user's mobile device Send Push notification
- d) ID server sends access symbol to the Internet service
- e) Internet service displays the required access symbol

- 2 The user receives an automatic notification of the authentication request on the user's mobile device. The user opens the notification or the SecSign app, selects the ID, and enters the PIN/passcode or scans the fingerprint. Then the user selects the correct access symbol among the symbols shown in the app.**



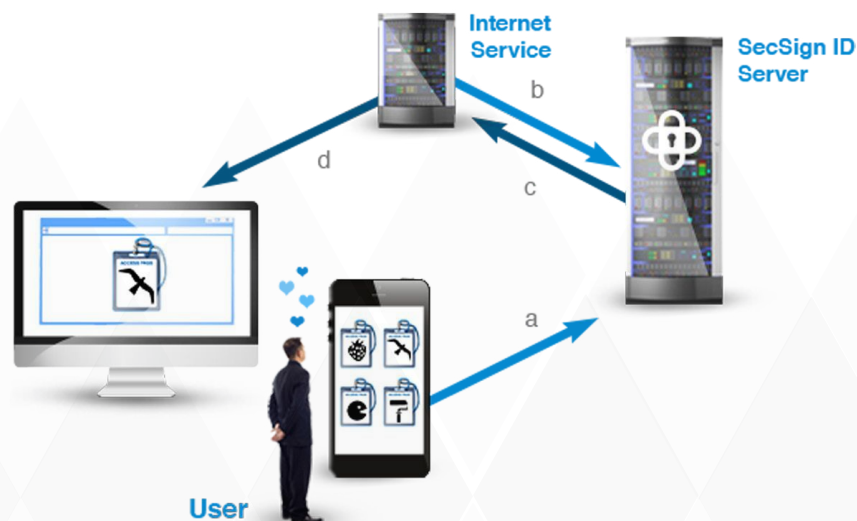
The diagrams shows the messages which are exchanged between mobile device and SecSign ID server.

What Happens During This Step:

The user selects the SecSign ID using a mobile app and enters a PIN.

- a) Mobile app confirms that the user is the owner of the SecSign ID
- b) ID server sends access symbols to the mobile app

- 3 The SecSign ID server verifies the result of the challenge-response procedure and, in the case of a positive result, releases the access symbol. The user is successfully authenticated and is granted access by the protected web portal, application, or service.**



The diagrams shows the messages which are exchanged between mobile device, SecSign ID server and Internet service

What Happens During This Step:

- a) The User confirms the correct access symbol and the mobile app sends this to the ID server
- b) ID server confirms access permission
- c) ID server sends access symbol to the mobile app
- d) Web service grants user access

The SecSign ID server manages only the user's public key that was transmitted securely via TLS encryption during the generation of the keys. The associated private key is unknown to the SecSign ID server. Thus, even if an attacker could access and read the public key that is administered by the server, the attacker would not be able to use it to log in on behalf of the user. Without the required private key, it is impossible to log in and authenticate access.

Authentication Procedure in Detail

The SecSign ID is immediately available to the user for logins after its generation. To log in, the user enters the SecSign ID on the website or through the login for the service or application that the user is attempting to access. The protected service sends a request to create an authentication session to the SecSign ID server. First of all, the server verifies whether the indicated SecSign ID is locked. If the ID is locked, the login will be rejected. Otherwise, the server proceeds to the next step.

In the next step, the server verifies if there is already an active login session for the same SecSign ID. In this case, both login sessions will be stopped and the SecSign ID would be frozen as a precaution. This prevents the user from accidentally accepting the login of an attacker who might have started a login at the same time with the same SecSign ID of the user.

The "frozen" status is automatically ended after a few minutes. The user can reactivate the SecSign ID immediately by selecting it in the SecSign app and authenticating. If the attacker continuously generates new login sessions (allegedly on behalf of the user) and thus interferes with the login of the user, the user is shown a priority code in the SecSign app, which the user can enter instead of the ID on the website. The user can even log in with it when the SecSign ID is frozen.

If the SecSign ID is not locked and there is not already an active login session for that ID, the SecSign ID server assigns an ID as well as an access symbol to the login session. This access symbol is defined at random, but it will never match the symbol used in the previous login session. If the previous login session was cancelled, the generation of a new login session is delayed by some seconds in order to prevent an attacker from quickly getting a session with a specified access symbol.

The SecSign ID server returns the access symbol to the website, application, or service that requested the login. The website, application, or service then shows the symbol on the login screen and asks the user to confirm the login in the SecSign ID app on the user's mobile device.

The SecSign ID server records the generation of the login session in the database and sends a push notification to all mobile devices containing this SecSign ID.

The mobile device shows the push notification with information about the website for which a login was requested. The user only has to tap once on the notification in order to open the SecSign ID app. The user then taps on the ID associated with the login request and is

prompted to confirm the login. According to the settings for this SecSign ID, the user either enters PIN or passcode or uses the scan of the fingerprint. For additional access protection, it is also possible to combine the PIN/passcode and the scan of the fingerprint.

The SecSign app decrypts the private key with the entered password or PIN. If a fingerprint was configured as the only access condition or no access protection is configured, then the random 16 bytes which were stored in the key chain for encryption will be used for decryption.

The decrypted private key is used by the SecSign app in order to send a get-pending-session request to the SecSign ID server. The SecSign ID server detects that this message type may only be executed after the authentication. For all these message types the following challenge-response procedure is used:

The SecSign ID server sends a 128-bytes long, random challenge value to the SecSign app. If the SecSign ID is, however, locked due to several unsuccessful authentications, the server will send an error message. For unlocking, the user must then replace the key of the SecSign ID with a new one by using the SecSign ID app.

The SecSign ID app generates an SHA-256 hash value through the challenge value, completes padding according to PKCS#1 v1.5 for the hash value, and creates a signature for this by using the private key. Then the SecSign app returns the signed challenge value to the SecSign ID server, which verifies the signature. If it is valid, the server will reset the counter for successive unsuccessful authentications to 0. Otherwise, it will increase it by 1. The counter for the total amount of unsuccessful authentications of this SecSign ID's key will also be increased by 1. If one of the two counters reaches its configured maximum (10 by default), the key of the SecSign ID will be temporarily locked. However, a login with other devices on which other keys for the same SecSign ID exist is still possible as the counters are independent from each other. Thus, a user can have the same SecSign ID configured on multiple devices and can still successfully log in with an ID, even if one of the devices has been lost or stolen and an attacker is attempting to use the ID on the compromised device.

After a successful challenge-response authentication, the SecSign ID server processes the request of the SecSign app. In case of a get-pending-session request, it sends a reply to the SecSign app. The reply contains the session ID, four access symbols, the name of the service that requested the login, and an optional message containing text.

The SecSign app shows the user the four access symbols, the name of the service and the message text (if applicable). In the app, the user taps on the access symbol which matches the symbol shown on the login screen for the service that the user is attempting to access. If the user selects an incorrect symbol in the app, the app will show an error message and will cancel the login after a second error.

If the user selects the correct icon, the SecSign ID will send an authentication-session request to the SecSign ID server.

The server verifies whether the login session has an acceptable status (e.g. it does not meet criteria for cancellation) and resets the session status to "authenticate". Alternatively, the user can reject the login in the SecSign app. The SecSign app would then send a corresponding message to the server. The mentioned messages are processed by also using the above mentioned challenge-response authentication.

The service that requested the login is requesting in the meantime the status of the login session in regular intervals from the SecSign ID server. It receives either the reply that the session has already been authenticated or cancelled, if an error occurred, or if a user action is still pending in the SecSign app.

1.2.3. Patented SafeKey-Procedure: Defense Against Brute Force Attacks Against the Key

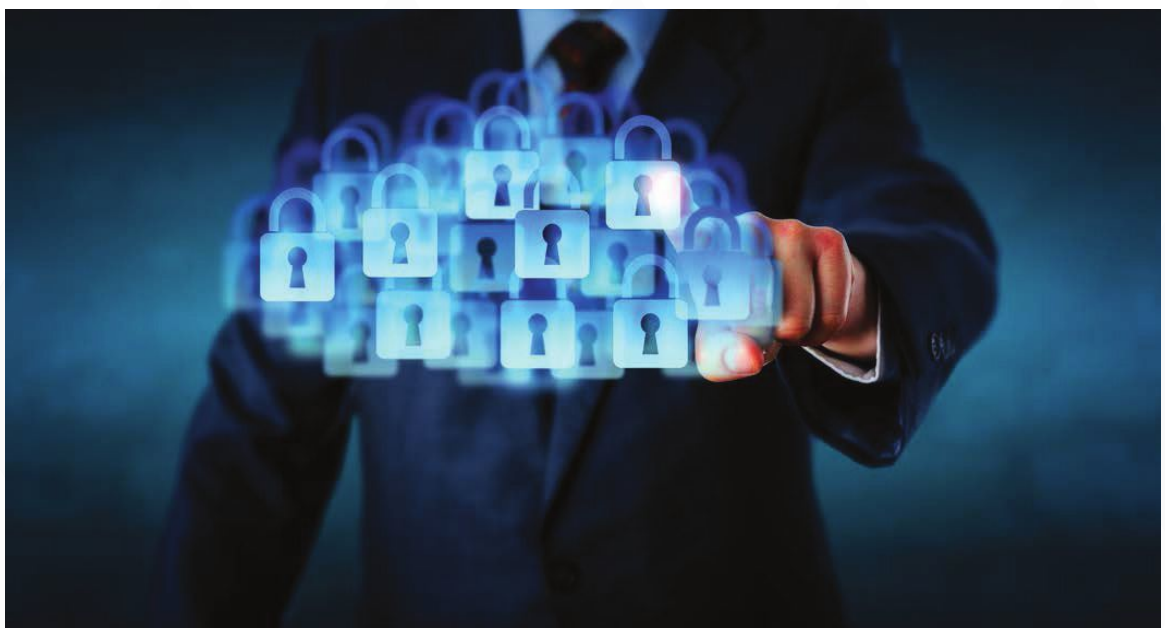
The common way to store keys is in formats like PKCS#8. But this represents a weak point security because an attacker might be able to test possible PINs, passwords, or passcodes and see from the format type of the decrypted data whether the string was correct. The SecSign ID, however, uses the patented SafeKey procedure (U.S. Patent No. 8,719,952). In this case, the key has no detectable structure. So, even if an attacker could somehow guess the PIN or passcode and “decrypt” the key, the attacker cannot detect whether the “decrypted” data represents the real key or not. Only the result of the challenge-response procedure with the ID server can provide this information. The ID server, however, will lock the SecSign ID after 10 unsuccessful login attempts (or fewer attempts if you specify this on an on-premise SecSign ID server). For a brute force attack, an attacker would need many more than 10 attempts in order to successfully guess the PIN or passcode. Thus, any brute force attack is doomed to failure.

1.2.4. Key Change

After continuous entry of the wrong PIN, passcode, or fingerprint, a SecSign ID will be locked from authentication. In order to use the ID again, the ID owner must generate a new key pair on the user’s mobile device. During this process, the private key on the mobile device and the public key stored on the SecSign ID server will be replaced. After the change of the keys, the ID can be used again.

The same procedure is used for the transfer of an ID to a new mobile device. SecSign ID allows a user to use the same ID on a new device or on multiple devices by adding the ID to additional devices and creating new key pairs for each installation. Thus, each device will always be configured with a unique pair of asymmetric keys to ensure total security across devices for that ID.

At any time and for any reason, the user can always access this feature and use it to generate a new pair of keys. The old keys will be invalidated by this procedure and will no longer be usable. The key change is authenticated with the above mentioned challenge-response-procedure in the same way that it is used for a login session.



Also, the SecSign ID app requires a key change if the app and its ID has been transferred together with the private key to another device by the use of an iTunes backup.

For unsuccessful authentication attempts during a key change, the server uses a separate counter. If the configured maximum number of attempts is reached (10 by default), the SecSign ID will be irrevocably locked.

1.2.5 Restoring a SecSign ID after Loss of a Mobile Device

If a SecSign ID user's device is lost or stolen, there is an ID restoration feature available to restore the ID on a new device. Optionally, a user ID can be restored on a new device by using an encrypted iTunes backup. For enterprises operating their own SecSign ID server, these two restoration options can be enabled or disabled for users. For more information about on-premise deployments of a SecSign ID server, please see section 1.6 of this document, SecSign ID Server as an On-premise Solution.

To activate the restoration option for future use in case of a lost or stolen device, the user must enable restoration in the SecSign ID app and provide a valid email address where the SecSign ID server will send an email verification code in the future as part of any requested ID restoration process. When the restoration feature is first activated, the SecSign app shows the user a restoration code which is generated by the SecSign ID server. The user should write down this code and store it safely in a secure place, so it is accessible in the future if the user's device is lost or stolen. For maximum security, both the restoration code and a separate email verification code will be required as part of any future restoration request.

If the user wants to restore a SecSign ID or add another instance of that ID on a new device, the user enters the SecSign ID user name along with the restoration code into the SecSign app. The SecSign app sends both of these to the server for verification. The server sends another, temporary code to the email address of the user. The user then enters this code in the SecSign app. The SecSign app generates a key, much like the initial key generation procedure for the SecSign ID, and sends the public key together with the temporary key to the server. The server now registers the public key in its database and, if the correct code has been entered, assigns it to the SecSign ID. The user can now use the SecSign ID on the new device.

1.2.6 Locking and Disabling an ID

If the user wants to lock the SecSign ID on a lost device or stolen device, or for any other reason, this can be done once the new instance of the ID has been successfully added to a new device. The user can then view a list of all devices where the SecSign ID is installed. The user can select any devices in the list and delete the assigned public key on the SecSign ID server. Thus, without the corresponding public key on the server, the SecSign ID private key on the lost or stolen device cannot be used, and an unauthorized authentication can never occur.

Independent of the restoration feature, the user also has the option to irrevocably disable a SecSign ID on the admin website of the SecSign ID server. So, if the user has lost or misplaced the restoration code, the user's ID can still be disabled. This can also be used in a case in which a device has been stolen and the user believes that the PIN or passcode has been compromised. With the admin website option, no restoration code is needed.

The SecSign ID server sends a code to the user's registered email address, and this code allows the user to disable the ID irrevocably.

Of course, as an added precaution, users who have enabled the "remote wipe" option in iOS or Android can remotely wipe all data from their mobile devices, including the SecSign ID app and its private key.

1.2.7 Using the SecSign ID on Several Devices

If the user wants to use the SecSign ID on several devices, this can be done by using the same restoration feature and process explained in 1.7.5 above, including enabling the restoration feature, adding a valid email address, and securely noting the restoration code for future use.

Once the user needs to configure a SecSign ID on an additional device, the SecSign ID server handles the procedure in the same way as restoring an ID in the case of a lost or stolen device. The user must enter the SecSign ID and restoration code in the app and then receive the email validation code and enter it in the app for additional verification.

SecSign ID then creates a new pair of asymmetric keys for the new instance of the ID on the additional device, but the ID will continue to function on the original device with its own unique pair of asymmetric keys. This process can be repeated in order to configure the same ID on an unlimited number of devices.

1.3 PROTECTIVE MEASURES OF THE INFRASTRUCTURE

1.3.1. SecSign ID Server: Data Management and Reliability

The SecSign ID server manages all users' keys that are transmitted during key generation. If the users also indicated an email address during the generation of the keys, the email address will also be managed and used for sending messages to the users, if necessary.

For cloud deployments of SecSign ID, the SecSign ID server is operated in high availability environments and deployed redundantly in independent data centers in order to provide maximum reliability. On-premise deployments can be configured in a similar way. The client sends all ID requests to a defined server. If the server does not reply or does not reply in time, the client will send the request to a fallback server. Each instance of the SecSign ID server uses an independent database which is replicated in two different availability zones. Every newly generated or changed SecSign ID is replicated in all databases.

All changes for a SecSign ID, such as changes in the authentication failure counter, key changes, and locking or adding devices, are automatically replicated by the SecSign ID server on the optional fallback SecSign ID server. Both SecSign ID servers have the same roles (i.e. requests from websites, applications, or services and from the SecSign app can be sent to both servers). Neither of them is only in standby mode.

1.3.2. Firewall and SecSign Routing Server Protection of the SecSign ID Server

In the cloud, the SecSign ID server is protected against attacks by multiple firewalls and protocol filters. For on-premise deployments, the server can be configured to operate behind enterprise firewalls and filters.

A SecSign routing server can be installed between internet and SecSign ID server for the protection of the SecSign ID server against overload by maliciously sent and invalid messages.

The SecSign routing server examines the incoming messages and disassembles and reassembles them. This way, messages in an invalid format do not reach the SecSign ID server.

The SecSign ID routing server also translates older message formats into the current format for the SecSign ID server. This way, websites using an older API version and older versions of the SecSign app can continue to work even after the SecSign ID server has been updated and uses a new message format.

1.3.3 The SecSign ID Server is NOT a Web Server

The SecSign ID server is not a web server but a proprietary development which is operated in a sandbox on the server. Thus, it is not dependent on vendors or subcontractors and has no corresponding weak points. No script frameworks are used.

1.3.4 Integration for any Web Portal, Application, or Service

SecSign ID can be easily integrated with virtually any website, application, or service, and it can be deployed in the cloud for free. Plugins are ready to use as well as interfaces that enable integration within minutes.

For integration plugins, tutorials, and documentation, please visit the following page on our website: <https://www.secsign.com/plugins/>.

1.4. PRODUCT DIFFERENCES COMPARED TO OTHER SOLUTIONS:

1.4.1. Data Minimization (No Phone Numbers, SMS, etc.)

To register and use SecSign ID, no entry of a mobile phone number is required by the user, and no mobile phone number is ever shared with a service or transmitted over a network.



Also, the user does not have to re-type long or complicated SMS codes or one-time access codes on a smartphone or tablet.

SecSign ID authentication is also available virtually anywhere in the world via WLAN and WiFi, with no requirement for mobile network access in order to receive SMS or one-time access codes. Thus, users can avoid problems stemming from international travel with no network availability or no access to international phone service for SMS texting. There is also no need to carry or activate a phone card for international calling and no need to worry about international roaming charges. The use of the SecSign ID app requires only WLAN/WiFi access by the smartphone or tablet.

1.4.2 The Role of PIN / Password

The user does not have to enter the required PIN or passcode anywhere in the web browser or other login mechanism.

Access to every user ID is secured by high-level protection without requiring long, complicated passwords with alternating numbers and letters or special characters.

Users can choose whether they wish to use a PIN, passcode, and/or fingerprint to verify their identity in the app. With PKI cryptography, a short PIN is sufficient because it is only required to prevent unauthorized physical access to the smartphone or tablet and attempted misuse of the SecSign ID for authentication.

Neither PIN, passcode, nor fingerprint is ever transmitted over a network or stored on a server, and each serves only as a physical authentication factor for encryption of the private key. As an added layer of security, the applied SafeKey procedure protects the private key against brute force attacks.

1.5 UNIQUE FEATURES OF SECSIGN ID TWO-FACTOR AUTHENTICATION

1.5.1 Security of the Authentication Procedure

No confidential information is ever entered through the login mechanism when using SecSign ID, which is a unique feature and unparalleled advantage that makes SecSign ID vastly more secure than other forms of authentication that rely on passwords and the entry and transmission of other sensitive credentials.

By using sandbox architectures or, in case of Apple iOS, by an additional verification of all applications by an Apple employee, current smartphone architectures provide additional support for secure key storage.

With this procedure and all mentioned steps and actions, the user is protected against brute force hacking, phishing, and malware attacks. An attacker cannot get the relevant information in order to authenticate. And an authentication server running SecSign ID is a deterrent for attacks because there is no database of confidential user credentials stored on the server and that would provide cybercriminals with an incentive to attack it.

1.5.2. Single Sign-on

With password-based authentication procedures, users must manage many passwords and are therefore tempted to use the same password for multiple logins, applications, and services. This creates a huge security risk for the user and, if the password is used for business as well as personal access, also for companies and organizations. SecSign ID eliminates passwords and thus removes all of this risk. No password is transmitted to any provider or stored by a provider, and the same SecSign ID can be used as a single sign-on for a limitless number of logins, applications, and services. Even if users use their SecSign IDs for personal and business purposes, there will be no risk for the companies because there is no password or any other sensitive user credential that might be used for multiple logins.



The users can use their SecSign IDs for all services that offer access with the ID. Therefore, they do not have to remember a huge number of user names and passwords and can always use a single ID with the same PIN, passcode, or fingerprint that is entered only into the mobile app and never into a login. If preferred, users can also create multiple IDs in order to differentiate their access for any reason.

Also, in the app, the user's SecSign IDs (user names) are always visible and available. So the ID or user name can never be forgotten.

The SecSign ID server can also be integrated into existing architectures like LDAP, Active Directory and Kerberos and used as authentication server.

For more details, please contact our experts on support@secsign.com.

1.6 ID SERVER AS ON-PREMISE SOLUTION

Businesses and other organizations can provide their own SecSign ID server as an on-premise solution. In this case, the IDs are presented to the users with custom branding, including a company or organizational logo in excellent quality.

The SecSign ID server and the SecSign Portal server (see below) are platform-independent solutions. They support existing SQL database systems.

The SecSign ID app can be used for several SecSign ID Trust Center servers at the same time. For operating an on-premise solution, no separate administration or distribution of the app is required.

For more information, please visit <https://www.secsign.com/products/on-premise-solution/>

1.7. ADDITIONAL ADVANTAGES COMPARED TO COMMON AUTHENTICATION SOLUTIONS

The user needs one single app on the smartphone. No additional software or hardware or the installation of additional programs (e.g. on the computer) is required.

The SecSign ID app for smartphones and tablets is available for free in the AppStore (iPhone) and via Google Play (Android). There will be no license or maintenance charges for the user of the app. The SecSign ID acts like other apps. Thus, every non-IT expert can use the SecSign ID app without any problems.

SecSign ID can of course be used in addition to existing authentication procedures. For example, if access is secured by smart card login, it is possible to add a smartphone and tablet login option with SecSign ID without much effort.

1.8. SECSIGN ID SIMILARITY TO AUTHENTICATION WITH SMART CARDS

The security level of the authentication process with SecSign ID is similar to a login with a smart card, which requires the secure entry of the PIN. For both SecSign ID and a smart card, a minimum of two distinct authentication factors are always required. With a smart card, the user must have the card, which is a physical authentication factor, and must know the required PIN, which is a knowledge factor. With SecSign ID, the user must have a smartphone or tablet that contains the 2048-bit encrypted private key, which is the physical authentication factor. The user must also know the required PIN, which is the knowledge factor required to prove rightful ownership of the key and allow it to digitally sign the authentication request. SecSign ID extends security further, however, by providing the option to authenticate by using a fingerprint scan, which is a biometric authentication factor. In fact, for added security, each SecSign ID can be configured to require three-factor authentication by requiring the combination of the physical possession of the encrypted private key along, a PIN or passcode, and a fingerprint scan. Thus, user access can be protected with a combination of physical, knowledge, and biometric authentication factors.

Both smart cards and SecSign ID use challenge-response encryption procedures that provide extremely strong security based on the latest technologies. However, the crucial advantage of SecSign ID is that no further hardware is required. For using a smart card, the user must use a card reader in order to execute a login. Furthermore, the user must connect the card reader with a computer and install the corresponding driver software. All these requirements are eliminated by using the smartphone or tablet that users normally carry with them anyway.

SECSIGN PORTAL

SecSign Portal provides the user with secure file sharing, file storage, and messaging in a single application. With SecSign Portal, you benefit from highest security for your data and user access, with total protection and completely confidentiality in an easy-to-use solution that delivers convenience and high usability.

The high-performance and user-friendly web interface of the Portal is optimized for all common web browsers as well as for all mobile devices (tablets and smartphones). It offers perfect support for business and private individual use in the cloud.

The basis of SecSign Portal is the highly secure user authentication via SecSign ID, which protects the user's data against unauthorized access.

SecSign Portal ensures the protection of confidential data against attacks and intrusion. With this high level of protection, you can manage your data in the Portal and share it securely and confidentially with colleagues and third parties.

2.1. DATA SECURITY

Beyond its powerful user access controls through SecSign ID, the central element of the SecSign Portal is comprehensive data protection. All data and messages are transmitted in encrypted form and, on receipt by the Portal, they are stored in encrypted blocks in the database. At no time are any data or messages transmitted or stored in unencrypted form. Powerful encryption is applied at every moment of transfer and storage.

2.1.2. Six-eyes Principle

A multi-authorization encryption scheme is used to protect the Portal server keys. To access the server keys, the simultaneous approval of at least three authorized administrators is required. This way, there is never a risk of a single individual potentially endangering the security and confidentiality of data. This same "six-eyes" principal is applied equally in on-premise solutions installations of the SecSign Portal.

2.1.3 Protection of the Portal Server

In the cloud, the Portal server, in the same way as the SecSign ID server, is protected by multiple firewalls.

In addition, the software solution SecRouter is applied as a reverse proxy on the server side. The SecRouter solution provides management and routing of authenticated TLS sessions against the SecSign ID server.

By using a web application firewall, SecRouter, and the exclusive use of prepared statements, SecSign Technologies protects the Portal against attacks like SQL and OS injections.

Successive delay makes attacks via flooding and DDoS difficult.

In general, all access takes place via HTTPS. The client and server verify all certificates. Furthermore, all documents and messages are stored in encrypted form (AES256) on the server side.

2.1.3.1 Web Application Firewall

The web application firewall checks each request to make sure that required parameters exist.

This means that:

- ◆ Existing parameters may only be sent via mail (apart from external links)
- ◆ The relevant parameters, 'request' and 'secsignid', must exist
- ◆ The requested parameters must be valid
- ◆ The SecSign IDs must match
- ◆ For each request the parameter values must be consistent

2.1.3.2. Encryption in Detail (AES 256-bit Encryption)

On its first start, the SecSign Portal generates 32 random bytes using a pseudo random number generator which employs the Micali Schnorr algorithm. These 32 random bytes and the UTF-8 encoded string "obenHauptBeschutz5" are the input of a SHA-256 hash computation. The SecSign Portal uses the resulting SHA-256 digest as an AES 256-bit

KEY

All uploaded documents and the textual content of transferred messages are encrypted using this fixed AES-256 key in cipher block chaining mode (CBC) while the data is being received. Each CBC stream starts with an initialization vector which originates from the pseudo random number generator mentioned above. During the transmission between the browser and the SecSign Portal, all data are protected by TLS encryption using an asymmetric cipher suite in combination with either AES or 3DES. The documents are never stored in plain text.

In order to survive a shutdown of the SecSign ID Portal, the fixed AES-256 key is encrypted and shared among multiple trusted employees of SecSign Technologies for cloud deployments. The same shared secret mechanism is used in on-premise deployments of the Portal, where multiple authorized administrators must simultaneously approve access to the key.

On each start, the SecSign Portal creates or assembles the fixed AES key. Then, 32 random bytes are generated to serve as an ephemeral AES-256 key. This ephemeral AES-256 key is subsequently used to encrypt the fixed AES-256 key in CBC mode. The encryption result is stored in a file in the file system of the SecSign Portal.

Then, the ephemeral AES-256 key is shared among trusted SecSign Technologies Inc. employees or an on-premise Portal's administrators using Shamir's secret sharing threshold scheme. Currently, there are eleven such employees that share the key for cloud deployments of SecSign Portal. The threshold of the secret sharing scheme is three. Hence, three employees or authorized administrators will be required to reassemble the fixed AES-256 key.

Each of the aforementioned authorized individuals has a special mobile device application holding a private key stored in the SafeKey format. The application generates the employee's key pair on the application's first start. The description of the SafeKey format has been filed as a patent application. The respective public keys of the employees are embedded in the


signed license file of the SecSign Portal. The SecSign Portal only accepts the license file, if it contains a valid electronic signature of a trusted developer of SecSign Technologies Inc. New versions of the SecSign Portal can only be uploaded to the server via an encrypted SSH connection by trusted administrators. The SecSign Portal now encrypts each share generated by Shamir's secret sharing scheme with the public key of the respective administrator and saves the encrypted result in a file in the file system of the SecSign Portal.

On the next start of the SecSign ID Portal, the administrator who has started the SecSign Portal process informs the trusted employees that they shall decrypt their shares in order to reassemble the ephemeral AES-256 key. To achieve this, at least three of the trusted employees run the special mobile device application which requests the encrypted share of the respective employee from the SecSign Portal. The application then decrypts the share using the private key of the employee and sends the result back to the SecSign Portal. TLS encryption is used whenever messages are being transferred between application and SecSigner Portal. The cryptographic routines verify that the TLS certificate of the SecSign Portal has been issued by a trusted certificate authority. The application further checks that the certificate's subject contains the DNS name of the SecSign Portal.

After having received three decrypted shares, the SecSign Portal reassembles the ephemeral AES-256 key, loads the encrypted file containing the fixed AES-256 key, decrypts it and is ready to encrypt and decrypt documents and messages. It then generates a new ephemeral AES-256 key and new Shamir shares as described above.



 2831 St. Rose Parkway, Suite 200
Henderson, Nevada 89052

 (702) 664 6467

 info@secsign.com

 www.SecSign.com