SSH.COM

Secure Signature

Version 3.11

Product Description

5.8.2021

THERE IS NO WARRANTY OF ANY KIND FOR THE ACCURACY, RELIABILITY OR USEFULNESS OF THIS INFORMATION EXCEPT AS REQUIRED BY APPLICABLE LAW OR EXPRESSLY AGREED IN WRITING.

SSH Communications Security Corporation
Karvaamokuja 2 B, FI-00380 Helsinki, Finland

Contents

1. Introduction

Secure Signature is a secure solution that enables you to get a contract or other file signed electronically. Depending on the use case, the document can be signed for example by hand, with a browser certificate or using bank identifiers. The solution also has the ability to check procuration.

Multiple people can sign the same agreement. Signatures can be made by multiple persons using the same terminal or each person signs the document in accordance with their own schedule. All signers are displayed in the finished document. It is also possible to forward a document for another person to sign, for example, in situations where a person does not have sufficient rights to sign the document.

The integrity of a digitally signed file can be checked. In addition, the Secure Signature solution makes it possible to see statistics on signatures and track the status of signature processes. A process can also be interrupted if necessary.

The product is fully responsive. With electronic signature the information is secure and can be electronically transferred directly to backend systems. To external users, the final signed document is always sent by secure e-mail.

Secure Signature features three components that make up the service and provide capabilities to start a signing process, sign documents and to manage ongoing processes. In addition to this, the users and configurations of Secure Signature can be managed through separate administrator tool (D-Center).

2. User interface

The user interface language is set according to browser's language settings. Supported languages are English, Finnish, Swedish, Danish and Deutsch.

2.1 Starting a signature process

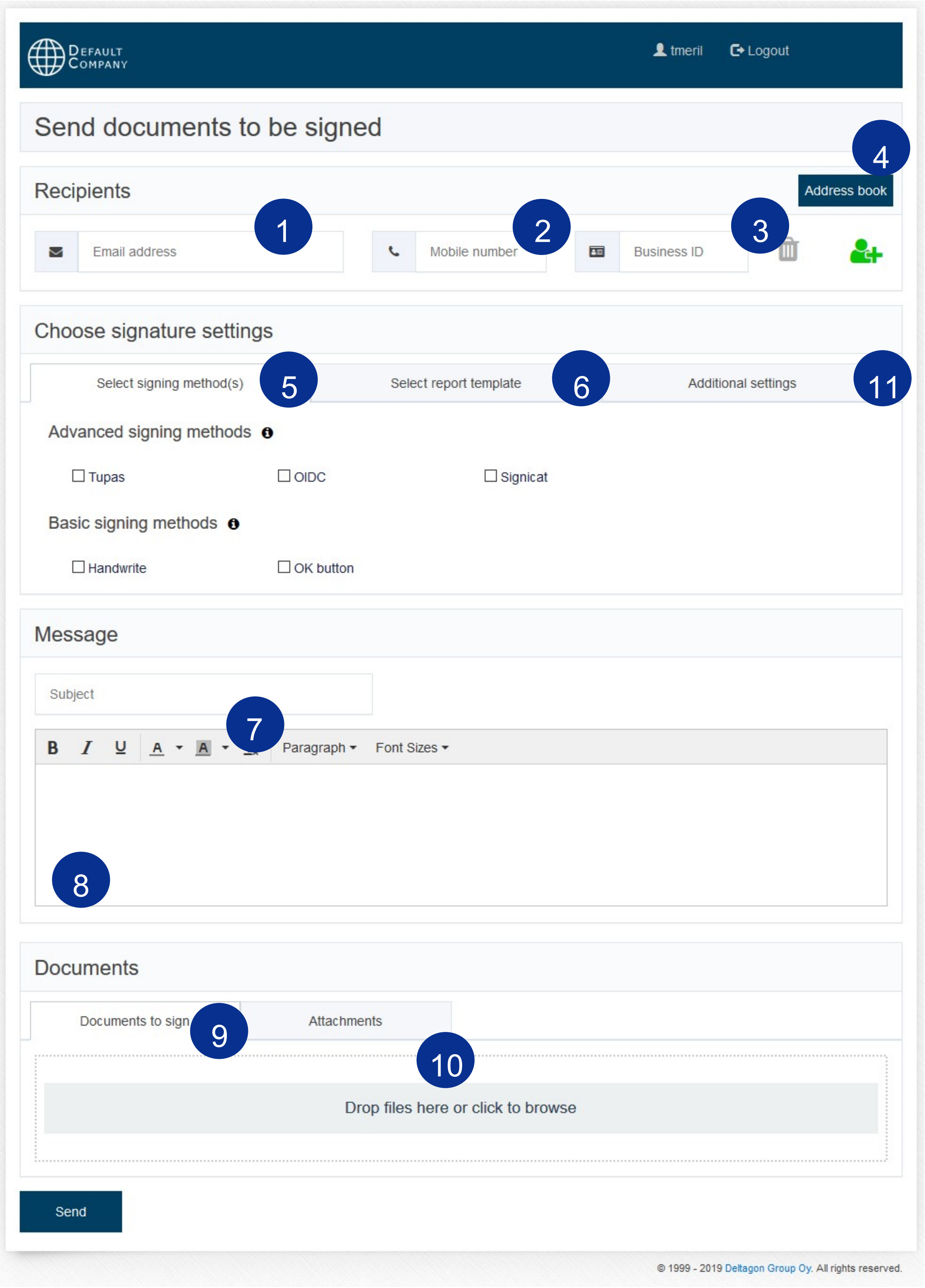
A secure signature process can be started in four different ways: from browser-based user interface, from e-mail using Sec@GW Outlook plugin, directly from a system in use via e-mail API or XML API or from collabRoom. The recipients will receive an e-mail message and a unique link to sign the document.

2.1.1 Web interface

Signature process can be started by using an interface that can be accessed through a web-browser. Alternatives shown in the interface depend on what options are enabled.

Please check the screenshots of the Web interface shown in next pages. Each function is addressed with numbers to features described in this page.

User defines in the interface the signatories' e-mail addresses (1), phone numbers (2), if the recipient is to be identified by a pin code, and business IDs (3), if they want to verify the person's right to sign in real time from the SAT. Previously used signatories can be added via address book (4) if it is enabled. Signature method selection appears if the signature method is not forced system widely (5), this section contains authentication methods which have been enabled in D-Center. User can also choose a report template (6) for the signed document if it is to be archived in a specific way. User must give the process a title (7) and write a message (8), enter the documents (9) that need signing. The user can add attachments (10) and specify other settings under the additional settings tab. In additional settings (11) the User can add their own signature (12) to the document(s) and force the signature order (13). The user can also force signers to download documents before signing (14) and enable SMS-invitation/notifications (15).



DEFAULT COMPANY tmeril Logout

Send documents to be signed

Recipients

Address book

Email address

Mobile number

Business ID

Choose signature settings

Select signing method(s) | Select report template | Additional settings

Advanced signing methods

□ Tupas □ OIDC □ Signicat

Basic signing methods

□ Handwrite □ OK button

Message

Subject

B I U A A Paragraph Font Sizes

Documents

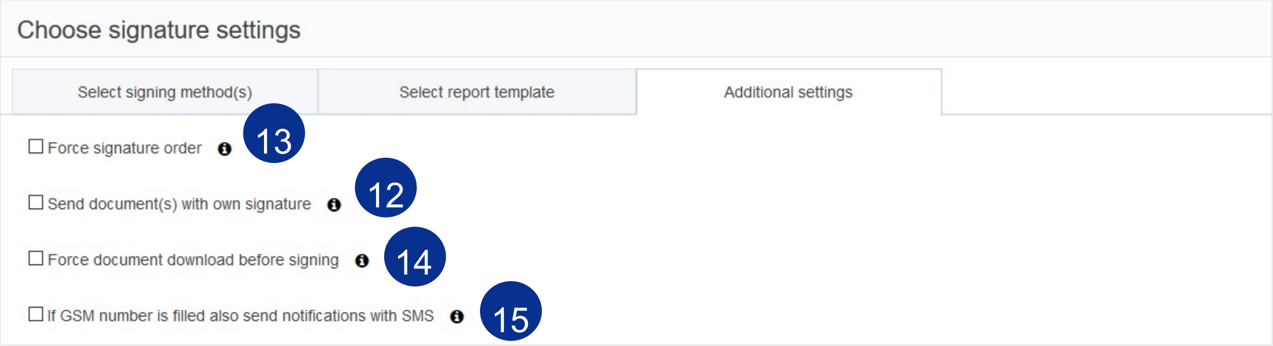
Documents to sign | Attachments

Drop files here or click to browse

Send

© 1999 - 2019 Deltagon Group Oy. All rights reserved.

Figure 1. Web interface to start a signing process



Choose signature settings

Select signing method(s) | Select report template | Additional settings

□ Force signature order

□ Send document(s) with own signature

□ Force document download before signing

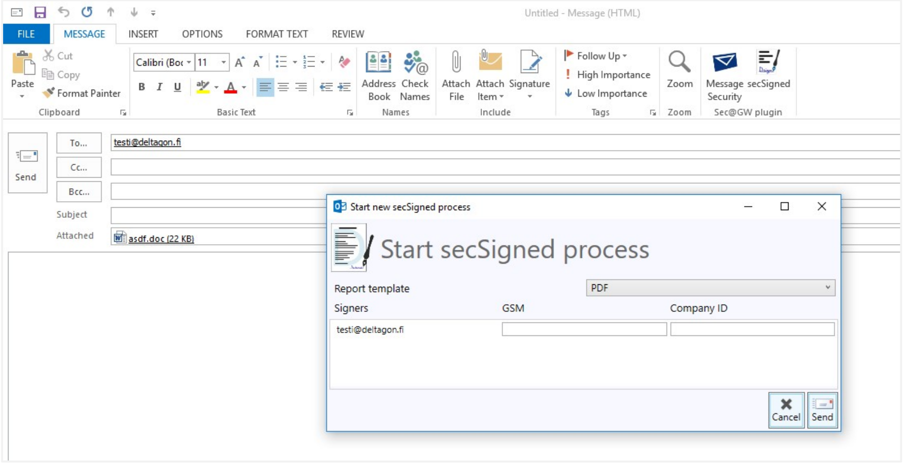
□ If GSM number is filled also send notifications with SMS

Figure 2. Additional settings in the web interface to start a signing process

2.1.2 E-mail interface with Sec@GW Outlook plugin

The signing process can also be started directly from the user's e-mail client with Sec@GW Outlook plugin. This requires the user to have Sec@GW e-mail encryption solution in use or configurations to email routing.

The plugin can be started either through the regular plugin pop-up by pressing the 'Secure Signature'-button or by accessing it directly from the panels.



Untitled - Message (HTML)

To... testi@deltagon.fi

Cc...

Bcc...

Subject

Attached asdf.doc (22 KB)

Start new secSigned process

Start secSigned process

Report template: PDF

Signers	GSM	Company ID
testi@deltagon.fi		

Figure 3. E-mail interface to start a signing process

2.1.3 Integration interface (XML API and e-mail API)

The signing process can be started directly from any system in use that can send XML request using the https protocol. For example, the process can begin by clicking a button in a CRM. The process can also be started from any system that can send e-mails with custom headers.

2.1.4 Integration to collabRoom

The signing process can be started from collabRoom and signed documents can be sent back to the same room the process was started from.

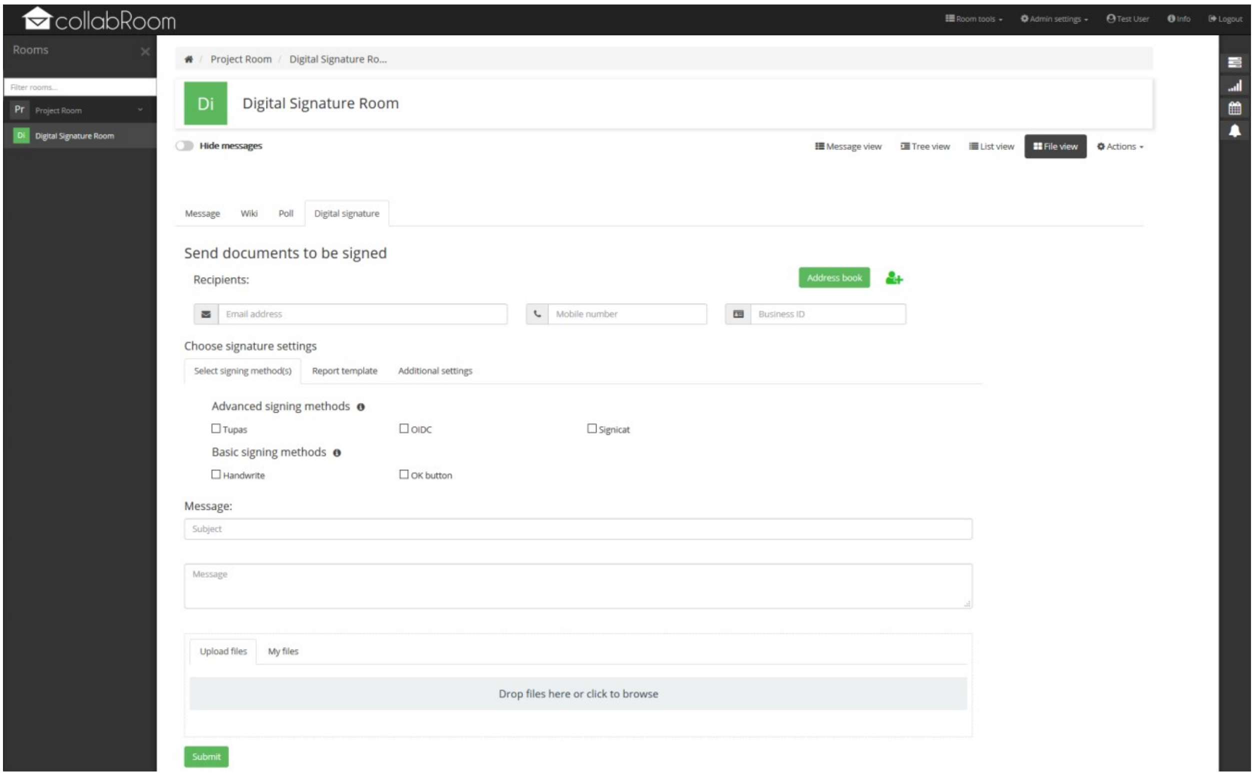


Figure 4. collabRoom interface to start a signing process

2.2 Signing documents

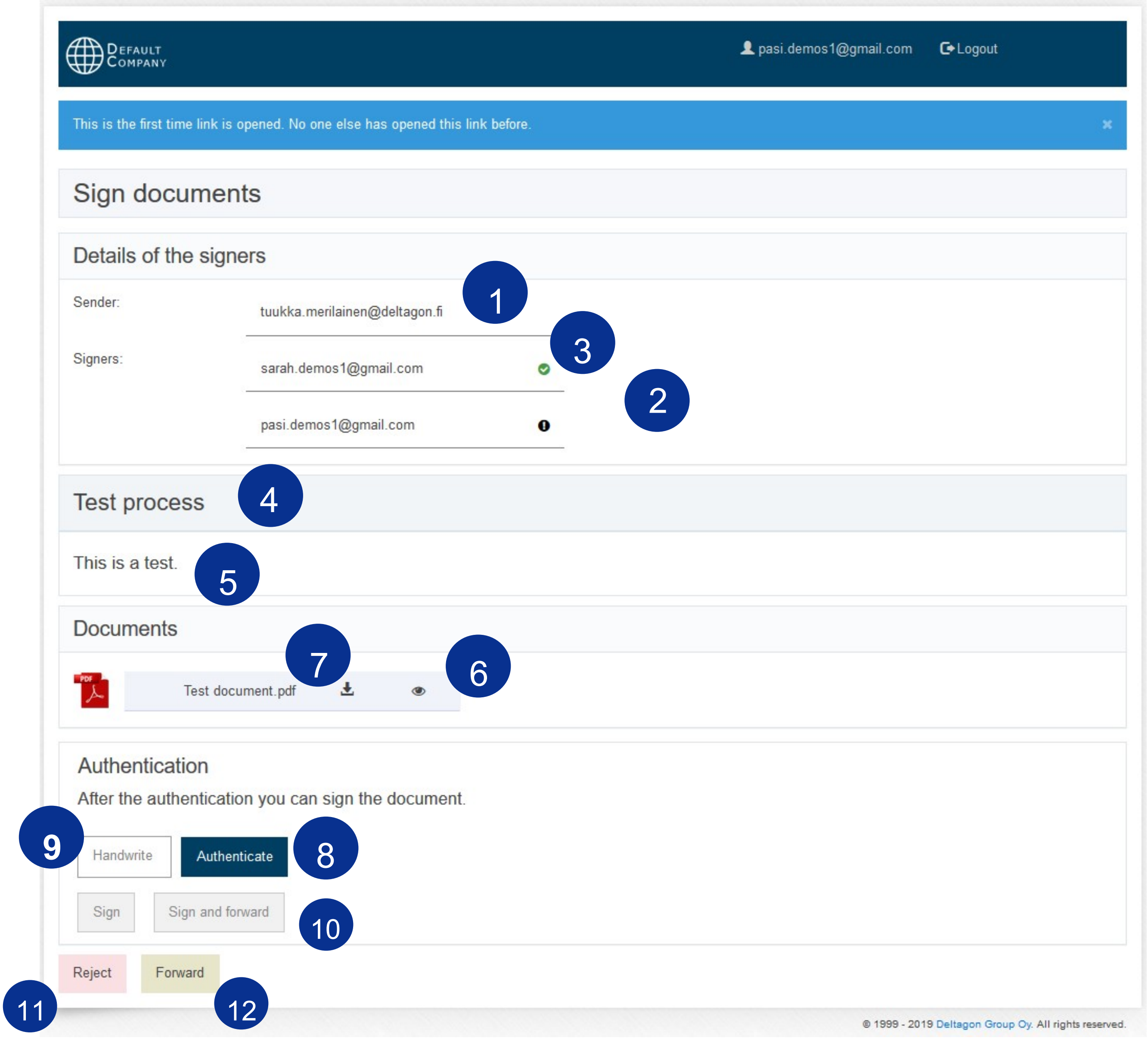
To view the actual signature invitation, the recipient opens a link received by e-mail. A pin code is asked if the sender has defined a mobile phone number.

On the signing page, the signer can see who started the signing process (1) and other possible signatories (2). If the process contains other signers who have signed already, a green icon will be shown next to signer’s email (3). A message from the process initiator will be shown (4 and 5) and signatories can view (6) and download the file (7) intended to be signed.

Depending on the enabled options, the signer can authenticate (8) by using the chosen authentication method (9) after which the documents can be signed or signed and forwarded (10) for another person to also sign.

If business ID has been added to the name, the person's right to sign is verified in real time from SAT (Suomen Asiakastieto) after the person has authenticated. User cannot sign the document unless they have the authority to sign in the company’s name.

The signer has the option to press reject (11) so that the entire process will be interrupted, and a notification will be sent for all parties involved. The signer can also be given the option to forward (12) the document to a designated person to sign.



This is the first time link is opened. No one else has opened this link before.

Sign documents

Details of the signers

Sender: tuukka.merilainen@deltagon.fi

Signers: sarah.demos1@gmail.com ✓

pasi.demos1@gmail.com

Test process

This is a test.

Documents

Test document.pdf

Authentication

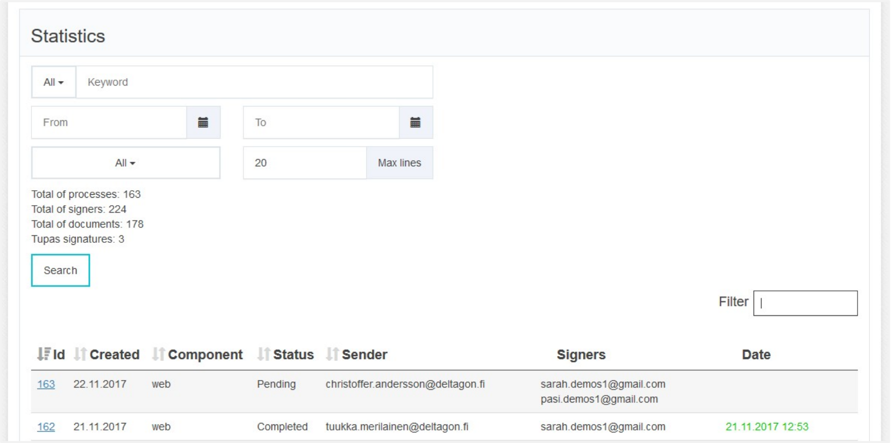
After the authentication you can sign the document.

Figure 5. Picture of signature page

2.3 Process Management

Secure Signature includes a management tool for overseeing both ongoing and completed signing processes. Statistic tool is a web based interface with separate user access. Through the interface it is possible to see user’s own processes or all processes.

By opening a process, it is possible to see detailed description of the state of the process, what signers have done so far, abort the process or send a reminder to involved parties that documents need signing.



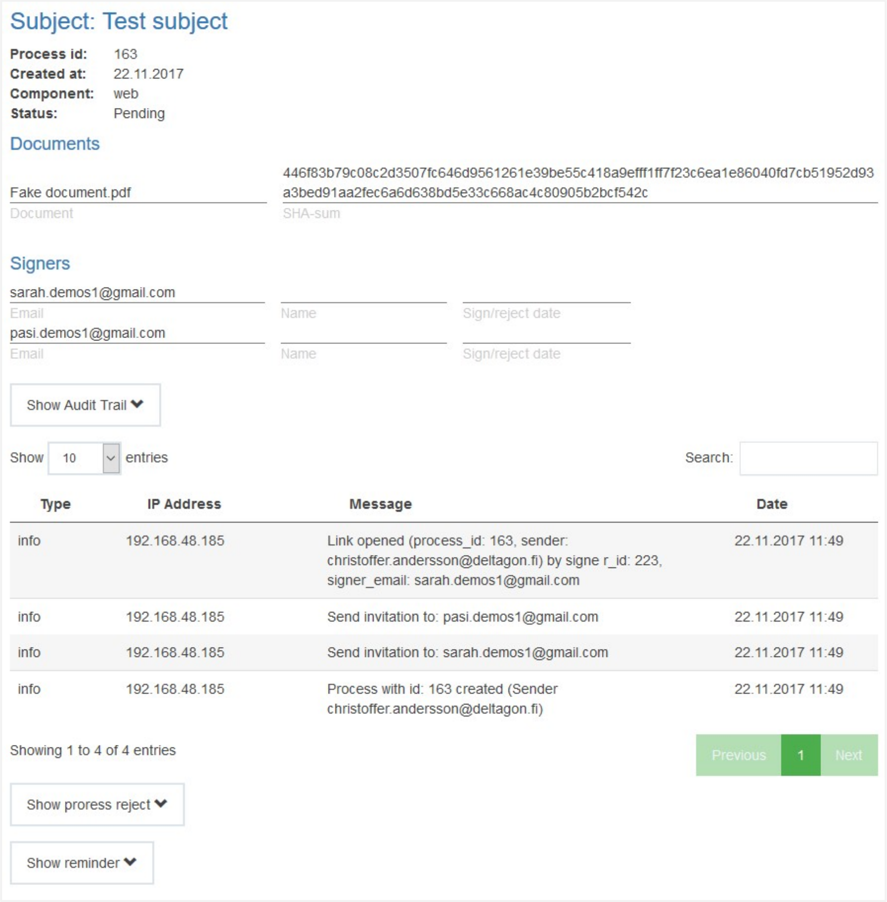
Statistics

20 Max lines

Total of processes: 163
Total of signers: 224
Total of documents: 178
Tupas signatures: 3

Id	Created	Component	Status	Sender	Signers	Date
163	22.11.2017	web	Pending	christoffer.andersson@deltagon.fi	sarah.demos1@gmail.com pasi.demos1@gmail.com	
162	21.11.2017	web	Completed	tuukka.merilainen@deltagon.fi	sarah.demos1@gmail.com	21.11.2017 12:53

Figure 6. Picture of statistics view



Subject: Test subject

Process id: 163
Created at: 22.11.2017
Component: web
Status: Pending

Documents

Document: Fake document.pdf
SHA-sum: 446f83b79c08c2d3507fc646d9561261e39be55c418a9efff1ff7f23c6ea1e86040fd7cb51952d93a3bed91aa2fec6a6d638bd5e33c668ac4c80905b2bcf542c

Signers

Email: sarah.demos1@gmail.com
Name:
Sign/reject date:

Email: pasi.demos1@gmail.com
Name:
Sign/reject date:

Show 10 entries

Search:

Type	IP Address	Message	Date
info	192.168.48.185	Link opened (process_id: 163, sender: christoffer.andersson@deltagon.fi) by signe r_id: 223, signer_email: sarah.demos1@gmail.com	22.11.2017 11:49
info	192.168.48.185	Send invitation to: pasi.demos1@gmail.com	22.11.2017 11:49
info	192.168.48.185	Send invitation to: sarah.demos1@gmail.com	22.11.2017 11:49
info	192.168.48.185	Process with id: 163 created (Sender christoffer.andersson@deltagon.fi)	22.11.2017 11:49

Showing 1 to 4 of 4 entries

Figure 7. Picture of process with opened audit trail

3. Administration

D-Center is the main administrative tool for Secure Signature where all available configurations are found.

Session settings

- User details (default: user agent): User agent can be used separately, with IP address or taken off completely.
- Session timeout (default: 7200 seconds): If the user does not refresh or request a page within the time-out period, the session ends.

Authentication settings

- **GSM maximum tries (default: 5):** Sets the limit for failed authentication tries for users with the GSM authentication method. If the user exceeds the limit the user account will be locked. The locked user account can be unlocked via D-Center’s Secure Signature User Editor.
- **Password maximum tries (default: 5):** Sets the limit for failed authentication tries for users with the password authentication method. If the user exceeds the limit the user account will be locked. The locked user account can be unlocked via D-Center’s Secure Signature User Editor.
- **Password settings:** The minimum length of password (default: 8) can be determined. In addition, to increase security, it can be required that the password must contain at least one lowercase letter, uppercase letter, number and special character. Users can also be allowed to order a password reset link (default: allowed).

Authentication: SMS-settings

- **SMS settings:** Setting for SMS authentication can be defined: length of PIN code (default: 4); the PIN may include numbers (default), letters or both; and maximum amount of PIN orders (default: 5 in 2 hours).
- **Forced GSM number (default: off):** The recipient GSM number can be made mandatory so that all recipients must be identified with PIN code proviced via SMS message.
- **Enable address book on process start (default: on):** The address book will appear for the user who is initiating the process from the web interface. This setting includes the possibility to define system-wide “global addresses” which can be added via D-Center. By default, all addresses which have been involved in previous signing processes will be shown in the address book for 180 days. Addresses saving period can be configured via D-Center.
- **Disclaimer page (default: off):** Before the signing view can be seen, the user can be shown a disclaimer about the confidentiality of the content. The disclaimer text can be customized and localized for each supported language.
- **Signer organization name fiels (default: off):** If this option is enabled the user who is initiating the process from the web interface can define an organization name/person's position title for each signer. This setting contains three choices: “Disabled”, “Enabled” and “Enabled and signer can edit”.
- **Enable sending notifications also with SMS (default: off):** By default notification related to the signing process will be sent via e-mail. By enabling this option some of the notifications will be sent like normally via e-mail and additional SMS notification will be sent if signers SMS-number has been

defined. This setting contains three different choices: “Not enabled”, “Allow sending notification also with SMS” and “Force sending a notification with SMS”.

Following notifications can be send via SMS:

- Signing request (invitation for the signer)
- Notification of the signature request that has been forwarded by other signers
- Notification about rejected process
- Reminder message for the signers to notify about a pending signature request
- Notification about completed signing process

Content of the SMS notification messages can be configured via D-Center in Secure Signature’s Template configuration section.

- **Show warning to the sender if only one signer is added and no own signature is given (default: off):** It is possible to show alert message for the user who is initiating the process from the web interface if only one signer has been added.
- **Allow process sender to add external appendix/attachment file which do not require signing, but which are related to the process (default: off):** By default all the files that have been added when initiating the process require signing. If the process should contain files that do not require signing (e.g. metadata-files or appendixes/attachments) this option has to be enabled. If this option is enabled the user who is initiating the process can add appendix/attachment files. When the user has added the appendixes/attachments there are two options: “Hide attachments from signers” (default) and “Show attachments to signers”.
- **Signature methods for signer (default: handwrite):** Supported signature methods are: Signicat OIDC authentication, Telia OIDC authentication, Mobile authentication, Suomi.fi, BankID (GrandID in Sweden, ZignSec in Sweden and Norway), NemID (ZignSec), chip card authentication (ex. HSTcard), certificate and by hand. Some authentication methods require a separate agreement with the service provider. GrandID, ZignSec, Suomi.fi and SAT interface also requires opening a port 443.
- **Allow process sender to select signing method when starting the process (default: off):** Signing methods have to be defined via D-Center (see the previous setting). By default, all signing methods that has been enabled will be shown to signers. If this configuration is enabled the user who is initiating the process from the web interface can select allowed signing methods per process.
- **Notification settings:** It is possible to send automatic reminders to people who have not reacted to the request. Invitation sender address and the number of days after which reminders will be sent can be defined.
- **SAT settings:** If procuration check from Suomen Asiakastieto has been taken to use, it is possible to define the time zone, user ID, password, MD5 key and test or production mode from D-Center.
- Logo file: Organization’s own logo can be entered. Logo will be shown in all pages of user interface.

3.1 User editor

Secure Signature does not require user accounts for the signers. To start a signing process or to maintain processes status user account is required. Administrators can add new or edit existing users. It is possible to specify the authentication method used for each user and if the user will have access to stats and if they can start signing processes. To create a new user the admin needs to enter the following information: username, e-mail address, clarification of signature and phone number.

- **Authentication methods for users:** User can be authenticated with a password, PIN code or user name only. It is also possible to make an IP restriction so that any company employees can initiate the process without a separate password.
- **Get users from LDAP (default: off):** Secure Signature can be integrated with company's AD system. User accounts are made from the e-mail addresses located in AD. Users with an attached phone number are created with pin-code login enabled. If user does not have a phone number attached, during initial authentication users must create their own passwords.

3.2 Group editor

In Group Editor Administrators can add and remove groups, add and remove users from the group, change privileges granted for the group and choose which report templates are available for the group members. A user can belong to one group.

3.3 LDAP Configuration Editor

Previously Secure Signature's LDAP configuration always required manual configuration on a console level. Starting from this version 1.9 LDAP configuration can be made via D-Center. Users that have been added via LDAP query will be shown in User Editor (see previous topic: User Editor).

3.4 Group editor

The look of Secure Signature interface and be edited through a custom CSS file. Also, all the default texts that are sent out during the signing process can be modified. These include invitations, reminders, process status checks and more.

3.5 Reporting options and report templates

Administrator can create new or edit existing templates for signing processes. It is possible to specify which is the e-mail address that the messages are sent from, if the signing page should be added as a separate file or made part of the pdf and in what language the report should be sent out.

Reporting templates can be named (eg. recruitment, NDA), recipients of reports can be chosen (email and/or http post), it is selectable in which format the reports are sent and a default template can be defined that can be forced on all processes or user can choose the template used.

- **Show signatures last in PDF (default: off):** Normally the signatures are shown on the first page of the signed document. It is also possible to define that they are shown in the last page of the PDF file.
- **Report language (default: Finnish):** Choose the language you want to receive your reports in. In addition, it is possible to create templates that use a specific language.
- **Final document report template (default: force template):** It is possible to force a default template or to allow users to choose the template they wish to use for each signing process.

3.6 Integration

Integration can be used to start the signature process or for reporting.

To start a process, integration is possible with e-mail or XML API to e.g. a file storage server.

- **Enable XML API (default: off):** To use XML integration the option must be enabled first. Define the API key and allowed IP address if needed.
- **Enable e-mail API (default: off):** To use e-mail integration the option must be enabled first.

Regarding reports, the final signed document can be sent to a defined URL with http post. In the XML based report, the documents are base64 coded. Other option is to send the report by secure e-mail (Sec@GW e-mail encryption is used).

4. Requirements in operational environment

4.1 Hardware and operating system requirements

Operating system is either RedHat Enterprise Linux 8 or Centos 8 with postfix –mail delivery system and Apache Web Server.

Recommended virtual hardware 4 -n CPU (2000MHz), 8 GB RAM, 146 GB HDD, two network adapters (if clustered).

Secure Signature is installed as a separate component to Sec@GW (version 3.7 and above).

4.1.1 Network connections and IP addresses

Servers are placed in to the network (typically to DMZ) Sec@GW server requires one to three public IP addresses. One IP address (eth0:0 adapter) will be used as a cluster address through which e-mail traffic is relayed. This IP address is used by the active machine. If NAT is used in address translation, information of both public and network address translated addresses is needed.

4.1.2 Cluster net (duplicated system)

Servers are in constant contact with each other concerning data and setting replication as well as automated monitoring. In order for the two servers to monitor each other, a dedicated connection is required (minimum of 100mbit full-duplex). Connection can be made with direct cable connection or connection through clutches. Usually, network uses addresses 10.0.0.20 (node 1) and 10.0.0.50 (node 2).

4.1.3 SMS interface

Users who log in using SMS authentication received a SMS message to the mobile phone. Sec@GW server creates an SMS message and sends it to the customer’s chosen SMS gateway in the net using email or http(s) interface. Next, customer’s SMS gateway sends the message forward to the receiver’s mobile phone.

4.1.4 Firewall settings

Firewall must allow the required connections. The following table shows requirements for basic installation; rules must be specified.

Table 1. Firewall settings

Connections to Sec@GW system (firewall settings)				
Port	Type	Source	Destination	Protocol / usage
443	TCP	*	Sec/c	HTTPS
25	TCP	Sec/c	* / SMTP GW	SMTP, shared messages
53	UDP	n1, n2	Nameservers	DNS
123	NTP	n1, n2	NTP servers	NTP
22	TCP	193.184.14.150	n1, n2	SSH, Reporting & updates, Deltagon's maintenance
443	TCP	n1, n2	193.184.14.150	Deltagon monitoring
443	TCP	n1, n2	193.184.14.151	Deltagon updateserver
80	TCP	n1, n2	Centos updateservers	CentOS updates
443	TCP	n1, n2	Redhat updateservers	Redhat updates

n1 = server 1

n2 = server 2 c

= cluster