Installation instructions

You have received the website seal source code via email (they come in two different types (samples below).

Please forward these instructions to your website administrator if you are not able to edit your website by yourself.

IMPORTANT: You can only display one type of website seal on your website at the same time.

Classic: The web seal is placed in an exact position on your website content and it moves with it when scrolling.
Insert the seal source code into the website source code wherever you want the seal to appear.

```
<!-- BEGIN SECUCERT SEAL BLOCK (CLASSIC for domain www.example.com) -->
<div class="CON_container_classic">
  <div id="con_s_container_14"> </div>
  <script type="text/javascript">
      /* <![CDATA[ */
      var _CONNET_ = document.createElement('script');
      _CONNET_.src = "https://verify.safesigned.com/seal_js?cert=14";
      _CONNET_.text = "var CON_14 = new CON(, 14, 5);
CON_14.loadSeal();";
      document.getElementsByTagName('head')[0].appendChild(_CONNET_);
      /* ]]> */
  </script>
  <noscript>
      <a href="http://www.safesigned.com/"><img

src="https://verify.safesigned.com/images/cert_14/seal/classic_js_disabl
ed.png"
          alt="SecuCert seal" style="border: 0" /></a>
  </noscript>
</div>
<!-- END SECUCERT SEAL BLOCK (CLASSIC) -->
```

SAMPLE

Tűzoltó utca 57., 1094 Budapest, Hungary
T: +36/1/299-2070, F: +36/1/299-2065
E: iroda_hungary@coface.com W: www.coface.hu

Floating: The content of your website scrolls underneath the web seal, making the web seal visible at all times.
Insert the seal source code on the website source code anywhere as the seal location is fixed (lower right corner of the browser window). We recommed you to insert the seal source code into the page header or footer. If you are using a separated file for header and / or footer (as an »include« file), then insert the seal source code into that separated file. The web seal will then automatically appear on every subpage of your website.

```
<!-- BEGIN SECUCERT SEAL BLOCK (FLOATING for domain www.example.com ) -
->
<div class="CON_container_rect">
  <div id="con_s_container_14"> </div>
  <script type="text/javascript">
      /* <![CDATA[ */
      var _CONNET_ = document.createElement('script');
      _CONNET_.src = "https://verify.safesigned.com/seal_js?cert=89";
      _CONNET_.text = "var CON_89 = new CON( 14, 5 );
CON_89.loadSeal();";
      document.getElementsByTagName('head')[0].appendChild(_CONNET_);
      /* ]]> */
  </script>
  <noscript>
<div style="height:40px; width:110px; z-index:10001 !important;
position:fixed;
          bottom:0px; right:45px; background-color:transparent;">
  <a href="http://www.safesigned.com/javascript-disabled.php"
style="height:40px; width:110px;
          display:block; text-decoration:none; background-
color:transparent;"><img

src="https://verify.safesigned.com/images/cert_14/seal/rect_js_disabled
.png"
      alt="SecuCert seal" style="border:0" /></a>
</div>
  </noscript>
</div>
<!-- END SECUCERT SEAL BLOCK (FLOATING) -->
```

SAMPLE

Tűzoltó utca 57., 1094 Budapest, Hungary
T: +36/1/299-2070, F: +36/1/299-2065
E: iroda_hungary@coface.com W: www.coface.hu

Exceptions

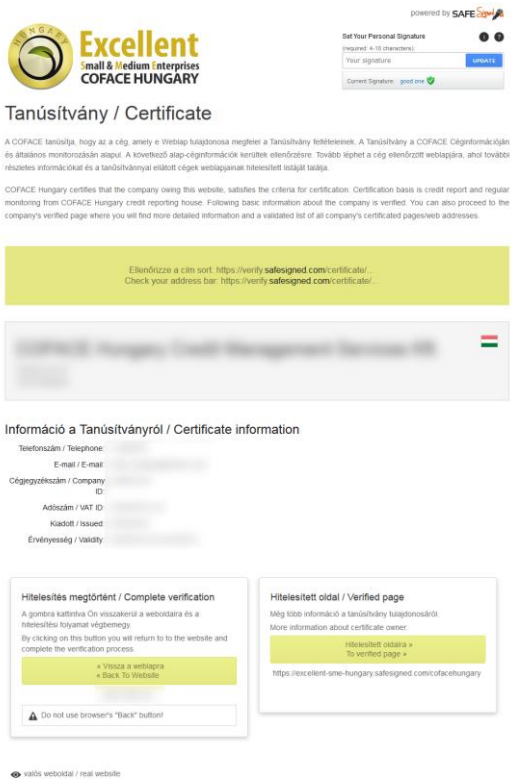
1. **CMS supported websites (WordPress, Drupal and Joomla)**
   These are three most popular content management systems.
   - **WordPress:** We suggest one of the two methods.
     1. **'Floating'** shape you may paste the code straight to (footer.php) as the code positioning is not important and the seal is always positioned in the bottom right corner of the browser.
     2. **'Classic'** shape needs to be inserted in 'Text' widget or any other widget that supports HTML/Javascript then include the widget where ever you wish to display the seal.
   - **DRUPAL:**
     1. Log on to your server via console (SSH) or cPanel or similar interface,
     2. locate the template file 'page.tpl.php' of your website. It is usually located in/sites/all/themes/templates/,
     3. open the file for editing,
     4. paste the seal code you received from the certificate issuer in the place where the seal needs to display,
     5. save the file,
     6. login to the site as site admin and clear cached pages.
   - **Joomla:** *Custom HTML Advanced* extension needs to be installed (http://www.pluginaria.com/custom-html-advanced.html). Seal code is then inserted into Custom HTML Advanced module, positioned anywhere on a Joomla supported website. You may also include 'floating' shape straight in the source code (head.php, footer.php …).

2. **Google sites and Wix**
   Google Sites and Wix have a very strong security policy concerning the external HTML/JavaScript code, which is in many cases removed immediately after the page is saved. So far we haven't been able to find a functional workaround.

3. **Facebook / Yellow pages sub-websites**
   Your Facebook / Yellow pages company page is in fact only a subpage of Facebook / Yellow pages website. SafeSigned seals protect the whole domain (for example www.facebook.com) and can therefore not be used to protect only one specific subpage of the Facebook / Yellow pages website.

Functionality

Website seal works only on a website it was issued for. Copying on another, non-authenticated website, is not possible. Click on a valid seal takes us to the website certificate which looks like this:



Certificate holds essential information about its issuer, owner, content description and navigation keys.

Left navigation key takes us back to the source website and the right one to the verified page.

Verified page contains similar information as the certificate itself. Verified page has a static URL address that can be as a company profile page.

Verified page URL is always composed in the following way:

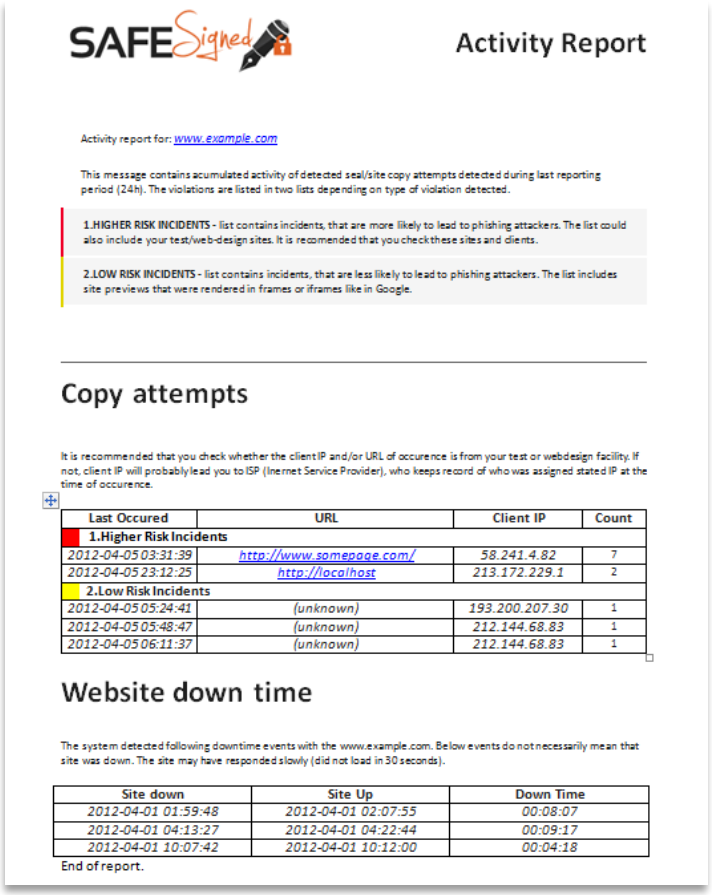
https://excellent-sme-hungary.safesigned.com/[CompanyID]

Tűzoltó utca 57., 1094 Budapest, Hungary
T: +36/1/299-2070, F: +36/1/299-2065
E: iroda_hungary@coface.com W: www.coface.hu

Technological features

»Excellent SME« certificate is based on SafeSigned technology. It proactivelly protects your website against unauthorised copying onto a different website server (phishing and copycat attacks). Additionally it monitors the accessibility of your website. Once a day you'll receive a daily summary report about the activities on your website via email, if there were any security events to report. This report is sent to the email address stated on the order form.

Activity report looks like this:



SAFESigned Activity Report

Activity report for: www.example.com

This message contains acumulated activity of detected seal/site copy attempts detected during last reporting period (24h). The violations are listed in two lists depending on type of violation detected.

1.HIGHER RISK INCIDENTS - list contains incidents, that are more likely to lead to phishing attackers. The list could also include your test/web-design sites. It is recomended that you check these sites and clients.

2.LOW RISK INCIDENTS - list contains incidents, that are less likely to lead to phishing attackers. The list includes site previews that were rendered in frames or iframes like in Google.

Copy attempts

It is recommended that you check whether the client IP and/or URL of occurence is from your test or webdesign facility. If not, client IP will probably lead you to ISP (Inernet Service Provider), who keeps record of who was assigned stated IP at the time of occurence.

Last Occured	URL	Client IP	Count
1.Higher Risk Incidents			
2012-04-05 03:31:39	http://www.somepage.com/	58.241.4.82	7
2012-04-05 23:12:25	http://localhost	213.172.229.1	2
2.Low Risk Incidents			
2012-04-05 05:24:41	(unknown)	193.200.207.30	1
2012-04-05 05:48:47	(unknown)	212.144.68.83	1
2012-04-05 06:11:37	(unknown)	212.144.68.83	1

Website down time

The system detected following downtime events with the www.example.com. Below events do not necessarily mean that site was down. The site may have responded slowly (did not load in 30 seconds).

Site down	Site Up	Down Time
2012-04-01 01:59:48	2012-04-01 02:07:55	00:08:07
2012-04-01 04:13:27	2012-04-01 04:22:44	00:09:17
2012-04-01 10:07:42	2012-04-01 10:12:00	00:04:18

End of report.

The first part of the activity report is called »Copy attempts«. All the events listed here mean, that there were copy attempts or editing events on your website. They are divided into »Higher Risk Incidents« and »Low Risk Incidents«.

Higher risk incidents list direct copy attacks over the website with seal. They detect also admin editing on the website, i.e. editing the website as its local / test copy. You can verify that by comparing the listed client IP with admin's workstation IP number.

We can determine the attack source by using the URL and client IP address. URL tells us the exact website address while the client IP tells us the access point of the alarm triggering device.

»Low risk incidents« mean, that your website was shown from a non-authorised IP address. Low risk incidents mainly include showing your website as a preview in a search engine, for example Google.

The second part of the activity report is called »Website Down Time«, which is basically a 24/7 monitoring over the website accessibility. It can be very useful to supervise the website server reliability, especially if you don't have the people (IT department) to take care of this and your company greatly depends on the accessibility of its website.