LeaderSSL®

Everything you need to know about Internet security and SSL-certificates

Contents

1. Free certificates: why you should not use them

Free certificates: why you should not use them

Free SSL-certificates are seemingly very profitable and easy way to protect your site. Indeed, why buy something when you can get it all for free from a variety of certification authorities? Free certificates attract business owners, but in the end its lead to losses. Why? Let's look further.

Free SSL-certificates are rarely trusted by major companies

In order for large corporations to include the root key of the CA (certificate authority) in own products, the CA must meet numerous conditions, the implementation of which requires significant financial investment. To attract such investments without the offer of paid products is virtually impossible. For this reason, the certification authorities that provide free certificates often have paid solutions in their product line, which differ in additional advantages: speed of issue, the possibility of including sub-domains, enhanced authentication, etc.

Free certificates are not suitable for sites which take payments

Free SSL-certificates rarely used to protect online stores, banks, websites, microfinance institutions, or any other sites accepting payments, because it is completely unclear who owns the site. People have less trust in sites protected by free certificates, which can have a negative impact on sales.

Free SSL-certificates are available mostly only as a DV (Domain Validation)

Free certificates are issued often only to verification by domain. Such certificates are not available for Code Signing, EV, etc. which vastly limits their use.

Free certificates: why you should not use them

Comparison SSL-certificates by brands

Comparative characteristic	Let's Encrypt	PositiveSSL	PositiveSSL Wildcard	Sectigo (Comodo) EV
Cost of issue	Free	$9,99*	$87*	$137*
Cost of reissue	Free	Free	Free	Free
Protection of the primary domain (1)	Yes	Yes	Yes + all sub-domains	Yes
Additional protection domain with «www»	Yes	Yes	Yes	Yes
Company name is displayed in the browser bar	—	—	—	Yes
Supporting subdomains	Yes	—	Yes	—
Display padlock icon	Yes	Yes	Yes	Yes
Trust Seal	—	Yes	Yes	Yes
Sales growth	No	Yes (minimal)	Yes (minimal)	Yes, up to 10-40%
Increase site positions in Google SERP	Yes	Yes	Yes	Yes
Suitable for	Non-commercial websites, blogs	Non-commercial websites, blogs	Site network of companies, organizations	Websites of banks, online stores
Type of validation	By domain	By domain	By domain	Extended validation
Mobile support	Yes	Yes	Yes	Yes
Insurance	—	Medium	Medium	High

Free certificates: why you should not use them

Comparative characteristic	Let's Encrypt	PositiveSSL	PositiveSSL Wildcard	Sectigo (Comodo) EV
Support by browsers	Only major browsers	All browsers (99.9%)	All browsers (99.9%)	All browsers (99.9%)
Length of the key	256bit	256bit	256bit	256bit
Encryption	SHA2	SHA2	SHA2	SHA2
Protection of pages from changes	Yes	Yes	Yes	Yes
Guarantee**	—	10,000$	10,000$	250,000$
		Recommended for individuals		Recommended for organisations

* When buying from LeaderTelecom: Free test period of 14 days – no need to enter credit card data or complete prepayments

** If the certificate is compromised, the certificate authority will compensate any expenses by the company and losses on the part of customers. With free certificates there are no guarantees and any losses will be taken up by you yourself.

All of this suggests that free SSL-certificates are “cheese in a mousetrap”. It is best to use proven paid solutions by known CAs. Prices on SSL-certificates are now available to all customers, which you can see on the LeaderTelecom site.

2. How to protect yourself from phishing: recommendations

How to protect yourself from phishing: recommendations

Anyone can fall victim to Internet fraud. If you are an online customer of a bank, or use their payment systems or make purchases on the web – please pay attention to these simple guidelines to help protect you from different types of online fraud.

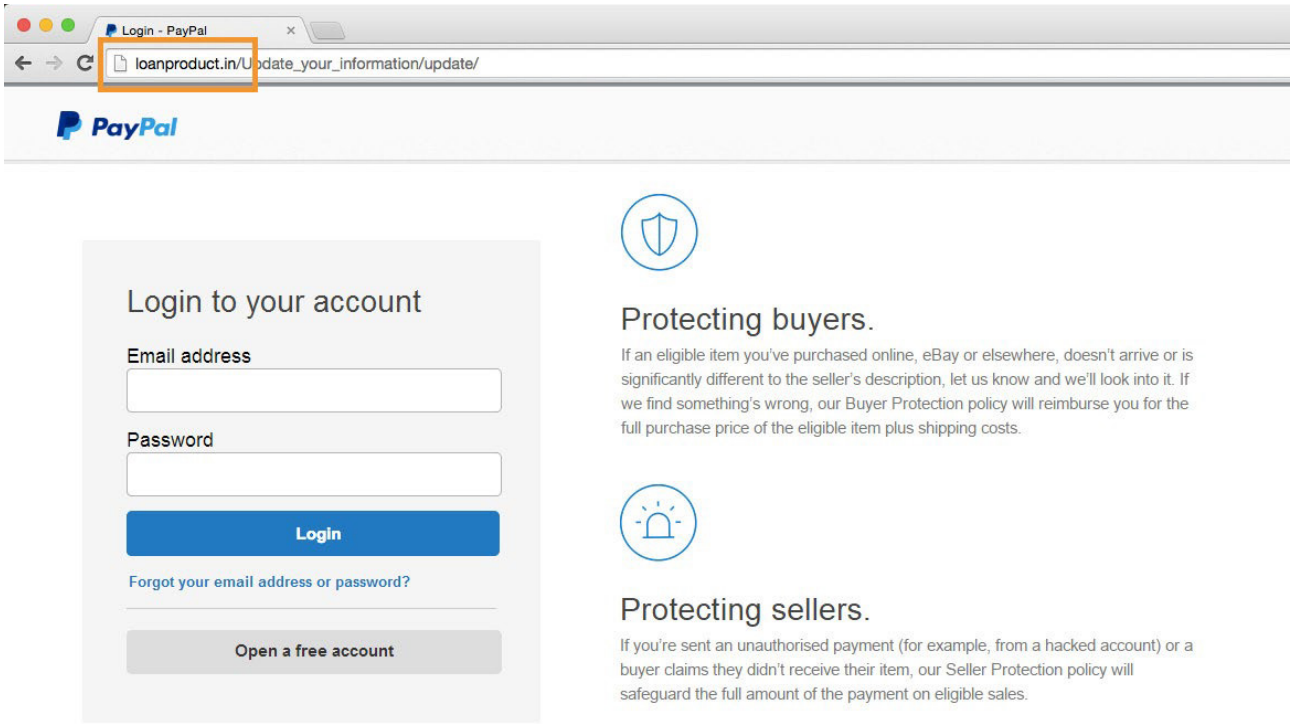
Phishing: how not to fall into the trap

Phishing is a form of Internet fraud, where hackers gain access to confidential user data, such as usernames, passwords and credit card numbers. Access to these types of data is obtained by specially created pages and sites that look very similar to the original. By entering data on such sites, users will help attackers gain access to important personal information.

One of the users of the payment system PayPal told us how he became a victim of fraud. When Roman wanted to get money from Forex, he accidentally moved onto a phishing site. As a result, he lost 100 thousand roubles that were stolen. Later Roman remembered that he did not turn on two-factor authentication via SMS and at the time of making the transaction Roman did not notice any differences from the genuine site. This illustrative example shows how important it is to protect your data in all possible ways.

Many phishing sites are virtually indistinguishable from the original. This is especially difficult when using mobile devices. How to determine whether the site is genuine and can you trust the site?

Example of phishing site



The first difference of phishing sites

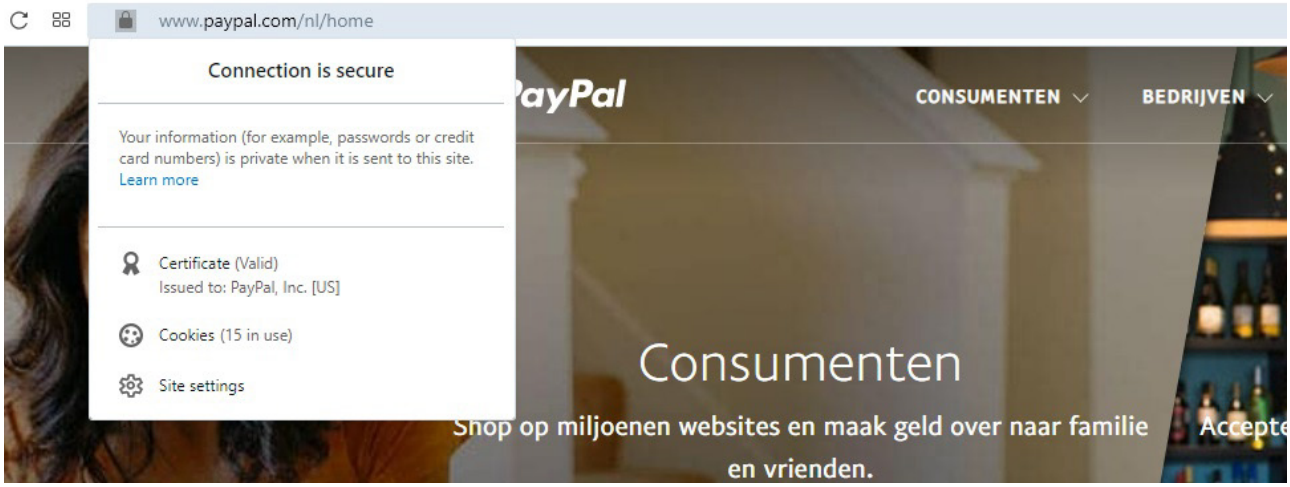
– URL (that is written in the address bar of your browser). So, there are many sites with URLs similar to https://paypal.com/. Many of these sites may not be available most of the time and activated only a few hours per day:

- **t.paypal.com**
- **paypal-visa.com**
- **paypai.co**
- **paypal.hk**
- **paypl.co**

Why do people visit such sites? Usually, the top positions in the search results take contextual advertising - paid links that may have nothing to do with the original service. You can easily fail to spot that the website URL is different, because the service name is similar to the genuine one.

The second difference of phishing sites - the lack of SSL-certificate. All pages where visitors are able to enter confidential information should use a secure https data transfer protocol. Most phishing sites are using insecure http, which means that such sites cannot be trusted.

When you go to a secure page, you can see the “Lock” icon, which appears in the address bar of browser. If you click on this icon, you will be able to discover information about the certificate.

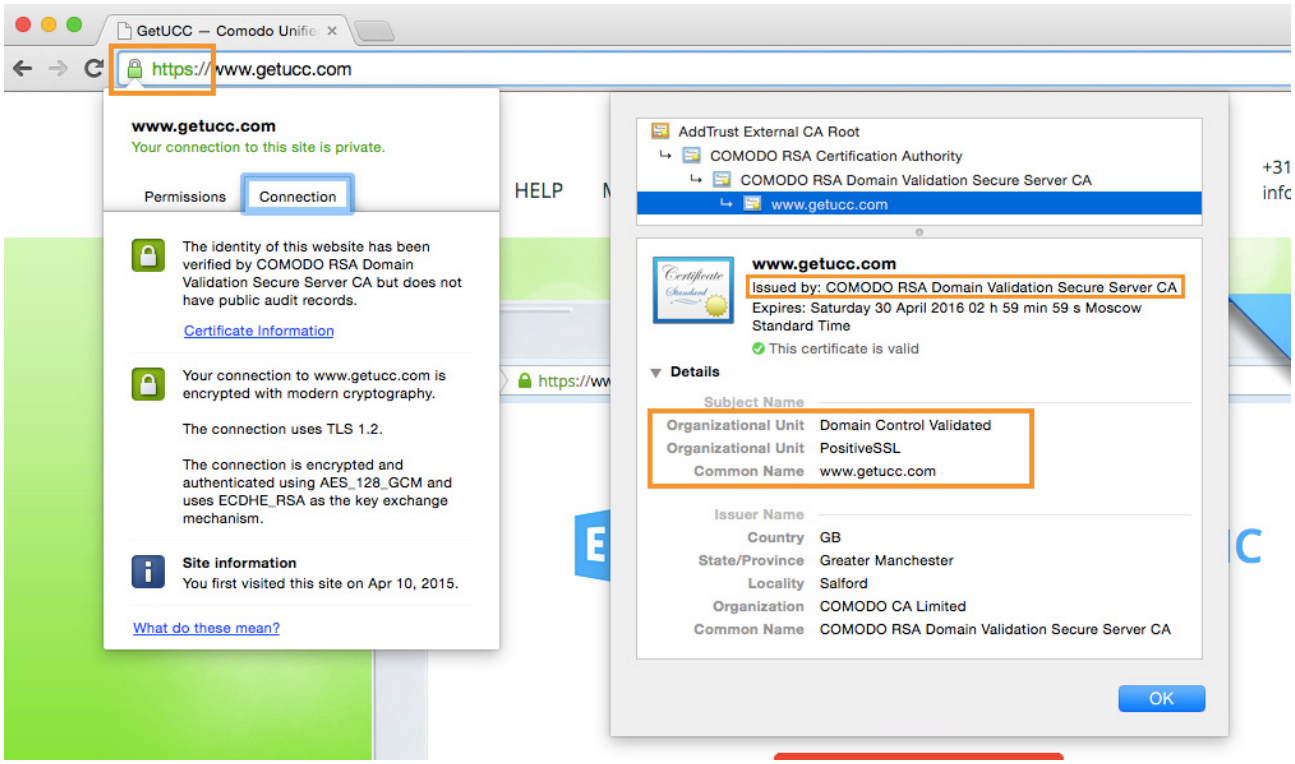


How to protect yourself from phishing: recommendations

Currently, there are phishing sites that use a secure connection with the icon “Lock”. In this case, you need to pay attention to the type of certificate: a DV-certificate will confirm only data protection on the phishing site, but no confirmation of the organisation itself (e.g. PayPal).

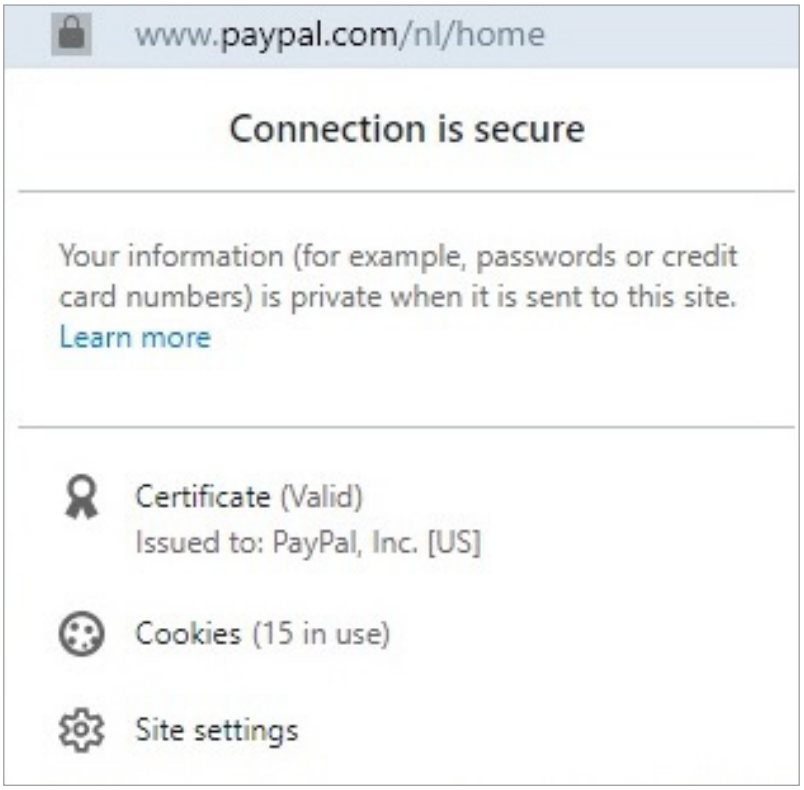
EV-certificate indicates secure connections. When you are clicked on the “Lock“ icon the name of the organization is displayed. EV-Certificates are the most trusted.

This type of certificate shows a company name and this, for the majority of Internet users, has long been a symbol and a guarantor of security.



SSL certificate: To help organisations

The correct step for any organisation whose activities are related to the processing of sensitive user data - is to acquire an EV SSL-certificate to guarantee security.



When using this type of certificate, all information is encrypted and is transformed into a set of characters that is useless to fraudsters.

For the organisation, the result of using EV SSL-certificate is sales growth of between 10-40% for all areas of Ecommerce, confirmed by independent researchers. You can order the certificate here.

For more information: https://www.leaderssl.com/products/ev

3. How to choose right certificate?

The difference between DV and OV certificates

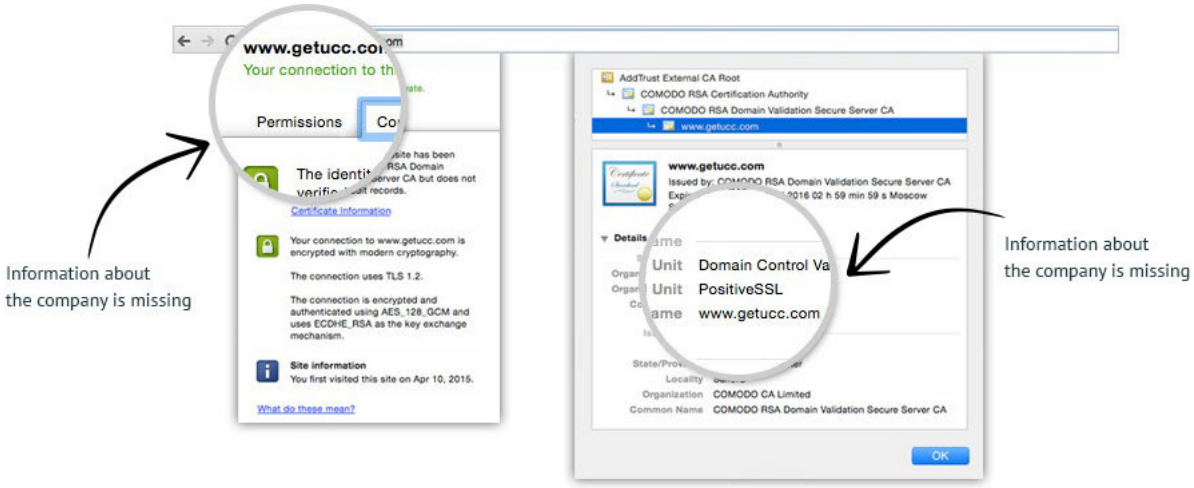
The difference between DV and OV certificates

We know that the SSL-certificates can be divided into three types: DV, OV and EV. In this article, we will focus on the first two types of certificates, DV and OV. We will explain how they differ and when you should choose DV over OV.

DV-certificates (Domain Validation)

This is the most basic level of SSL validation. The Certification Authority (CA) only ensure that you are the owner of a specific domain using the information contained in the WHOIS. Naturally, this type of certificate enables secure data encryption on your site, but it does not verify that you are the owner of a legitimate business. It is legitimate, and, most importantly, it is a very quick solution to protect your site using HTTPS. Customers seeing the padlock in your browser will have more trust in your site than before, because the padlock is a recognised sign of legitimacy.

Example of a DV certificate:



A DV certificate is fine where security is not a concern: however, attackers can also use DV-certificates on phishing sites. Unsuspecting users see the trusted pad lock and enter their personal data on the site which can then fall into the hands of fraudsters. The fact that the data channel is secured does not necessarily mean that the data will go to the right people. A user needs to be sure that the site belongs to a legitimate company if they are to make a purchase or input important information.

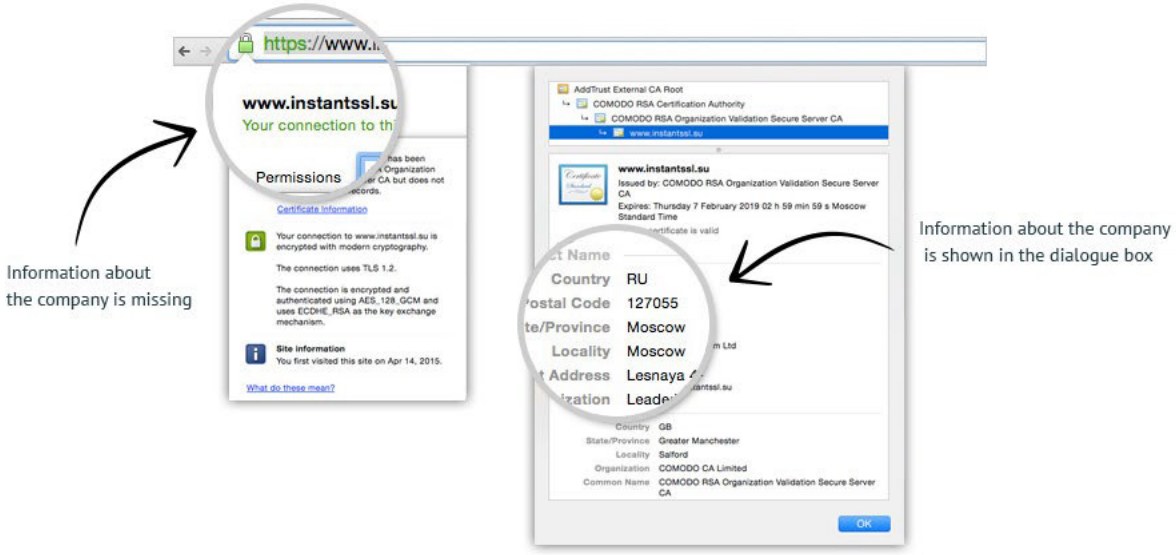
For this reason, if security is a necessity for your site, we recommend an OV-certificate.

The difference between DV and OV certificates

OV-certificates (Organisation Validation)

are required for companies and organisations where users must enter sensitive information (credit card numbers, contact information, etc.).In particular, they are useful for e-commerce sites or online sales. An OV-certificate authenticates the owner of the site and requires legitimate business information for that company. The validation process for these certificates is longer and more detailed. The Certification Authority not only verifies the fact that you own the domain, but also the fact that you are the owner of the company. The company must be in a business registry database and in a trusted online directory (for example, dnb.com). Fraudsters cannot get an OV certificate because their organisation cannot be validated. The main advantage of getting an OV-certificate is that your company will be listed on the certificate.

Example of an OV-certificate:



You should think about switching from a DV-certificate to an OV-certificate, if:

- **You need to protect sensitive user data**
- **You want to display your company name on a certificate (provides more trust amongst users)**
- **You are planning to expand the business and grow it to a new level**
- **You want people to know that the site is a legitimate organisation, and not a phishing site**

The difference between DV and OV certificates

If you want to switch from a DV-certificate to an OV-certificate, be sure to contact our experts at LeaderTelecom. Our knowledge, experience and streamlined process for dealing with the CAs will make issuing an OV-certificate easy and convenient.

More Information about DV SSL-certificates:
https://www.leaderssl.com/products/dv

More Information about OV SSL-certificates:
https://www.leaderssl.com/products/ov

4. How to choose right certificate?

The difference between OV and EV SSL-certificates

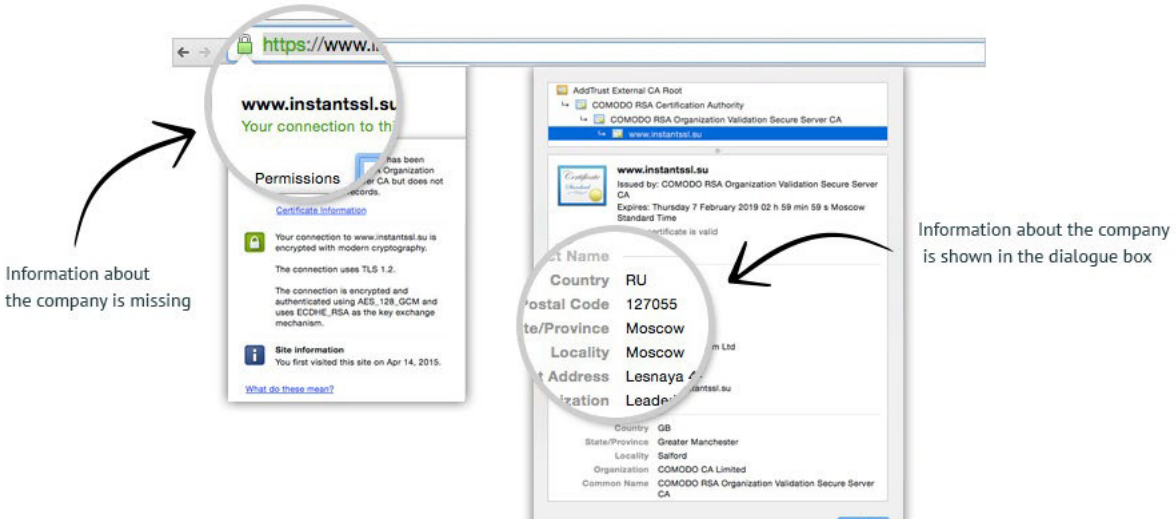
The difference between OV and EV SSL-certificates

Nowadays, SSL-certificates are an essential requisite for e-commerce. It is difficult to imagine that a credible business site would not be secure. Users simply will not enter confidential information on sites, even if they need to make a purchase. For this reason, the owner of any credible online business should be considering an SSL-certificate from a proven company. There is however, one question that needs to be considered first: what type of certificate is best to choose – OV or EV? What is the difference between these two SSL certificates?

OV-certificate (Organisation Validation)

OV-certificate (Organisation Validation) is a certificate that confirms the existence of the organisation. To get an OV certificate, the company must complete the validation process. During validation, the certification centre must ensure legal (reference to the state resource) and physical (reference to the trusted online catalogue) existence of the company. As a result, if the site is protected by an OV-certificate, the visitors will see a lock in the browser's address bar, which ensures that the site is protected from hackers.

Example of an OV certificate:

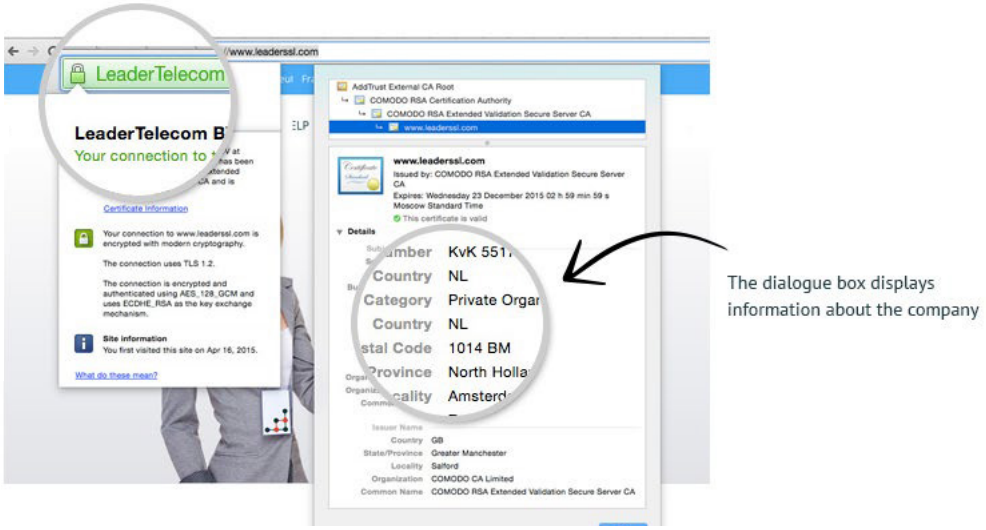


More information about OV-certificates: https://www.leaderssl.com/products/ov

EV-certificate (Extended Validation)

This is the most trusted and secure solution that is actively used by the world's leading online businesses. This certificate displays a company name in the browser bar guaranteeing security and reliability. Visitors can easily see that you are a legitimate organisation and not fraudsters. Getting an EV certificate is not much more complicated than getting an OV certificate, but it is a lot more trusted and secure. EV-certificates provide users with the confidence that your website is secure and this increased trust helps boost sales.

Example of an EV-certificate:



- EV-certificates include the name of the company (displayed in the browser's address bar) and some additional information about it
- EV-Certificates are not much more expensive than the OV-certificates, but have more benefits
- EV-certificates are used by most large organisations worldwide

If you are thinking of getting an EV certificate but think that the validation process is too complicated or too long, then look no further! Allow our professionals at LeaderTelecom to do this work for you. Our knowledge, experience and streamlined processes will help you easily acquire an EV certificate.

More information about OV-certificates:
https://www.leaderssl.com/products/ov

More information about EV-certificates:
https://www.leaderssl.com/products/ev

5. SSL-certificates for online stores: a necessary addition for online businesses

SSL-certificates for online stores

You have opened the online shop of your dreams, which already brings you some income, but you are trying to find ways to make it more profitable. What opportunities are there to increase the revenue that you're receiving? One of the most popular solutions is an SSL-certificate, which will allow you to sell more by increasing the confidence of potential buyers. An SSL-certificate brings three advantages:

- **It increases your income due to growing trust to your Web site**
- **it protects from theft the personal information of your customers**
- **it prevents the emergence of site-clones (or, as they are otherwise known, phishing sites) ***

SSL is a modern standard for virtually all online financial transactions.

Online stores are very difficult to imagine without using SSL, because they conduct various financial transactions that require entering sensitive user data. These sites are very vulnerable to theft of passwords, so they must be always be protected by SSL.

Professionals recommend protecting the entire online store, not just its individual pages with important data. This approach gives a lot of advantages:

- **Users immediately see that your site is protected - your browser has a lock and/or company's name in the address bar**
- **No one can steal valuable information from your customers (credit card numbers, postage addresses, user's personal data, etc.)**
- **Access to visitor statistics for analytical services will be closed (no one will know which pages your customer visited, what they bought, etc.)**

Which SSL-certificate to choose?

Today there is a wide range of SSL-providers: DigiCert, Sectigo (Comodo), Thawte, etc. If you are selling premium products, you might want to take advantage of DigiCert Secure Site Pro with EV SSL-certificate. In addition to it you will get a special Norton Seal trust logo, which is a sign of quality and security for any online store. It should be placed on all pages of the online store, as well as next to the login form, in order that the visitor understands that the site is under perfect protection.

** True only for SSL-certificate with a green address bar (EV-certificates).*

Why is it so important to display the trust logo?

The main advantages of displaying trust logo on site:

- **Users see that your site is secure, and therefore enter their personal information and make purchases.**
- **Norton - a recognisable brand, which in the minds of many people is associated with security software. The «Norton Secured» logo attracts additional trust from users.**
- **If a user hovers the mouse cursor over the logo, he will be able to see all the information about your company and the protective tools used on your website.**

If you need a cheaper solution, then in that case you can have the Thawte EV-certificate or a Sectigo (Comodo) EV-certificate. This EV-certificate allows the site to display a padlock and a company name in the address bar. The user will immediately notice a visual signal and realise that the site can be trusted, because it is protected.

OV SSL-certificate (Organisation Validation) is not recommended for use in online shops. This type of certificate allows you to put a padlock in the address bar of your browser, clicking on which will display information about the company. However, not all users are technically savvy enough to browse information about the company. Therefore, they might simply refuse to purchase on your site.

DV SSL-certificates allow you to display the lock in your browser, but do not contain data about your company. Thus, you will achieve the security of transactions on the site, but cannot defend against data theft via phishing sites. Hackers can get quite the same DV-certificate and create a fake copy of the online store, directing users to it and obtaining their data.

For these reasons, we strongly recommend to all owners of online stores to purchase EV SSL-certificate, which bears numerous marketing benefits and can reliably protect a site from intruders.

With this, the visitor receives a non-verbal sign saying that the site should be trusted (green is always associated with a permit). The user can immediately see who owns the site, because the company name is displayed in the address bar of their browser. The trust of visitors to the site will grow, and so the site's sales grows too. Statistics show that sales growth could be up to 10-40%.

Now some maths. Let' say your website sales reach 100,000 euros a month. We assume that sales growth will be 1% (minimum percentage). EV-certificates cost from 90 euros per year. We get the increase in sales for the year:

100,000 x 12 x 0.01 = 12,000 euros

Subtract the certificate cost of 90 euro.

Net profit amounts to 11,910 euros.

All of this indicates that the SSL-certificates are a very profitable investment which quickly pay for themselves. Another important factor in sales growth is brand awareness. The Baymard study showed that people are more likely trust the VeriSign (Now DigiCert).

Using standard EV-certificate, we have a profit of 11,910 euros.

Now let's look how to change the situation with the using of DigiCert certificate. The initial conditions are the same. The difference is that DigiCert is more prestigious and recognisable brand in comparison with many other certification authorities, and this EV-certificate costs 630 euro/year. In this case we get more visitors trust and higher likelihood that a person will complete their purchase.

In the case of DigiCert with an increase in sales of at least 3%, we get the following:

100,000 x 12 x 0.03 = 36,000 euros

Subtract certificate costs - 630 euro.

As a result, we have increased sales by 35,370 euros.

Calculation of efficiency of use of EV SSL-certificates for online stores

Without SSL-certificate	
Sales in the store (in euros).	100,000
With an installed SSL-certificate from a standard authority	
Minimum certificate price (in euros/year)	90
Minimum sales growth	1%
Sales growth (in euros)	12,000
Sales growth minus the SSL-certificate price (in euros)	11,910
With SSL-certificate DigiCert EV	
Minimum certificate price (in euros/year)	630
Minimum sales growth	3%
Sales growth (in euros)	36,000
Sales growth minus the SSL-certificate price (in euros)	35,370
Profit growth in the transition from standard EV to DigiCert EV	
Sales growth (in euros)	23,460
Sales growth (in %)	197%

Increase sales using DigiCert EV-certificates almost 3 times higher than in the case of standard EV SSL certificates.

For this reason, in Germany and United States many companies prefer the DigiCert brand.

Additional arguments in favor of the SSL-certificate:

- People often think that the site is secure only if it has a lock bar in the browser. This axiom is prescribed in many books and articles on security. Many people will leave the site, if they don't see a small padlock or company name while clicked on it. Thus, if you do not enable SSL for the entire site, you may lose a percentage of users. They simply think that your site is dangerous and will not buy anything on it.
- In August 2014, Google reported that the availability of SSL on each page of the site allows the growth of SEO ranking in search results. This was done as part of a campaign for Internet protection following some major data breaches. This is another plus in the arguments for SSL-certificate installation.
- Studies have shown that the percentage of purchases in online stores, protected with SSL, increases to about 40%. Users have a negative attitude towards sites with no padlock or company name in the address bar of the browser, and there fore go to competitors who have installed the SSL-certificate. As seen in a recent user survey, conducted by DigiCert Certification Authority, approximately 78% of the respondents are willing to shop online, if they see a padlock in the browser bar.

It is best to order the SSL-certificate from proven companies such as LeaderTelecom. We are a strategic partner of Sectigo (Comodo) and offer SSL-certificates from this certificate authority at the best prices.

Also, you can order DigiCert SSL-certificates which are ideal for doing serious business online.

About LeaderTelecom

LeaderTelecom is an ambitious company with a strong team. We love what we do and our members strive to create value for our customers.

The strategic goal of LeaderTelecom is to provide a high quality service in SSL and grow across the globe. An important component of our globalisation programme is to open offices in numerous countries around the world. The services provided by LeaderTelecom create significant benefits for our customers.

We will be happy to answer your questions and help you to make a perfect choice. Feel free to contact us any time:

http://www.leaderssl.com
info@leadertelecom.nl
+31 20 7640722