

ASRECO
DATA SYSTEMS

SSL certificates and identity crisis in the network



SSL Certificates

- ✓ Definition
- ✓ Function
- ✓ Types

SSL Certificates – Definition and functions

Definition

SSL Certificate – a cryptographic protocol ensuring the security of internet communication, compliant with the X.509 v.3 (RFC5280) standard
Its main function is to secure communication between the web browser and the web server.

Functions



Encryption – data transmission protection and assurance that requested or transmitted data is delivered without unwanted transformations

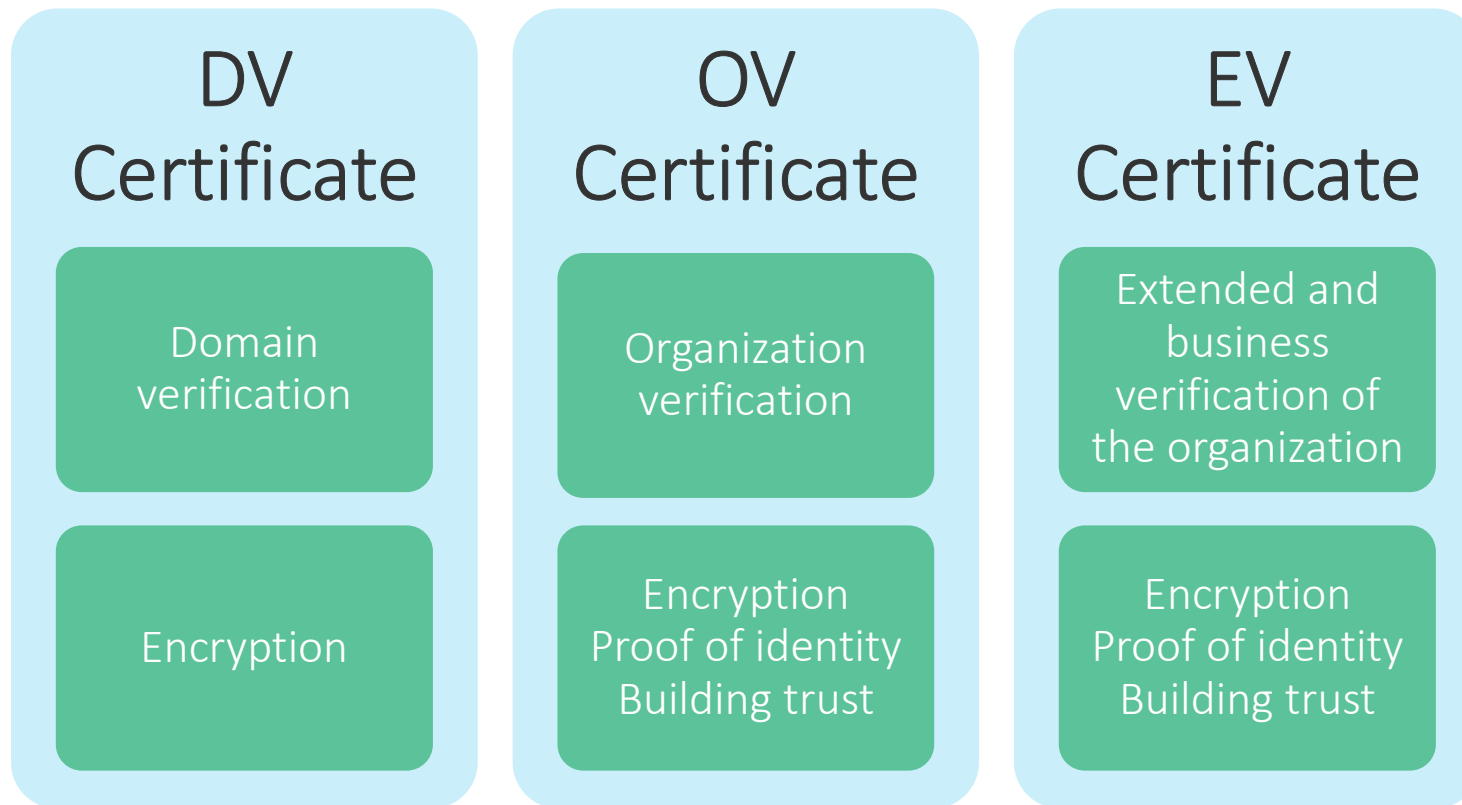


Authentication – ensure that the server you are connected to is in fact the correct server


















Building trust – emphasizing the transparency of the website for the Recipient and the possibility of presenting company data from the certificate level

Types of certificates



Types of certificates

	Domain verification	Organization verification	Business and operational verification of the organization	Highlight on the address bar / identity panel	Encryption	Building trust	Warranty
DV (Domain validation)							
OV (Organisation validation)							
EV (Extended Validation)							

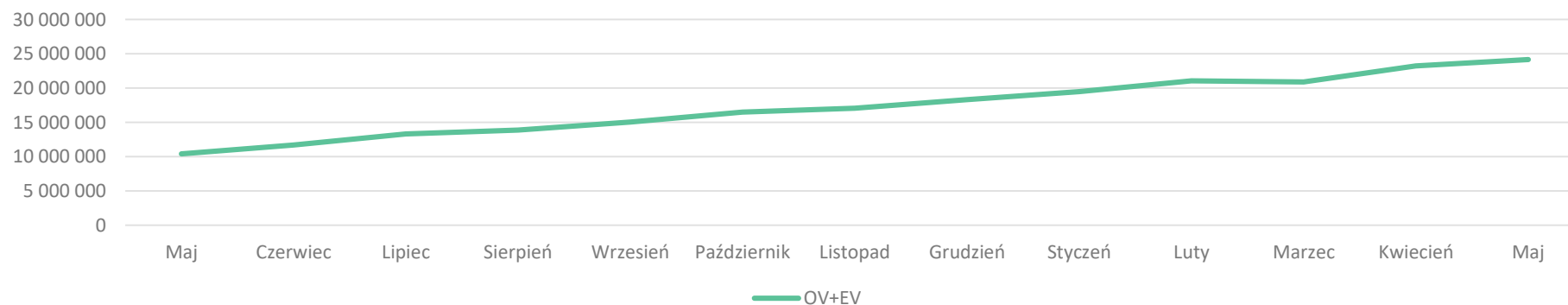


Current trends on the
certificate market
in the era of identity

Current trends in the sale of SSL certificates

The increase in sales of OV certificates results primarily from the desire to emphasize the company's identity on the Internet and draw the recipient's attention to the available level of data about the company. OV and EV clearly communicate the transparency of the website, indicating its origin.

Higher class certificates not only encrypt traffic, but also allow you to build trust.



• Source : <https://ssl.netcraft.com/surveys/analysis/https/2020/May/CMatch/certsfrm>

Advantages of OV and EV certificates

The strength of the OV and EV certificate has always gone beyond the green bar, as its essence results primarily from the detailed verification that the company undergoes before issuing the certificate.

Its advantages are :

- ✓ emphasizing that the company is legal;
- ✓ ensuring the identity of the company;
- ✓ allows less known brands to build their position and encourages customers to buy in-store;

Value of OV and EV certificates

Authenticity and building trust

Building trust and identity – Identity is the basis of digital security in the 21st century.

Value of OV and EV certificates

Protection against phishing



The most vulnerable websites will be without certificates or with DV certificates, which are the easiest for phishing criminals to impersonate.

Investing in a certificate with the highest validation is not only an investment in data encryption but also protection against phishing attacks.

Cyber Forensics Innovation Research Lab to Georgia Tech shows that the domain of EV SSL certificates are 99.99% free from abuse on the Internet.

EV	3	0,05%
OV	8	0,13%
DV	6009	99,82%

Value of OV and EV certificates

Compliance with regulations

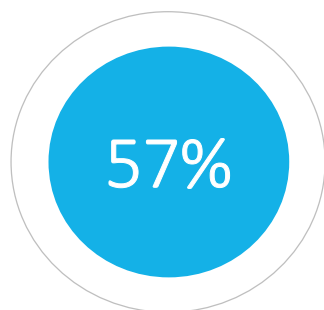
OV and EV certificates allow many institutions to achieve compliance with applicable law in terms of identity transparency, both in terms of European legal regulations and internal regulations.

This trend is indicated by new technological standards, such as, for example: [the amended Payment Services Directive \(PSD2\)](#) or [the requirements of the Federal Office for Information Security in Germany \(BSI\)](#).

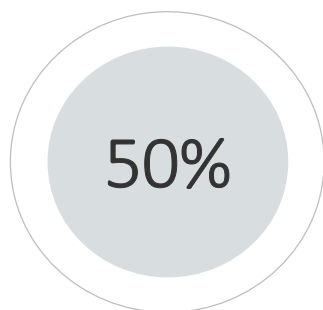


OV and EV certificates

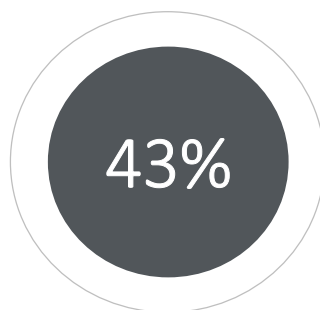
What do customers visiting the website with OV and EV SSL say?



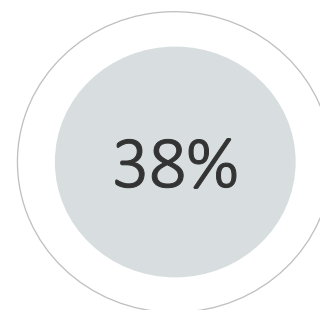
people are more likely to share personal data



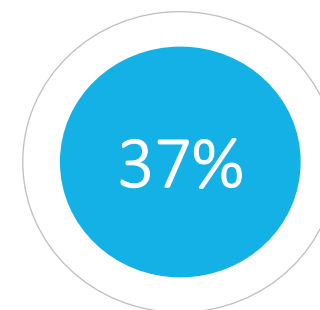
is more often involved in financial transactions



more often creates a new account



they are more willing to fill in and submit an online form



will make a purchase more willingly

• Source: Cyber Forensics Innovation Lab, Instytut Georgia Tech

Commercial certificates are synonymous with quality and safety

Thanks to continuous investments in the development of security infrastructure, commercial CAs represent the highest level of service quality and minimize the risk of a wrongly issued certificate almost to zero

Commercial CAs guarantee a high level of service and certificate maintenance. The owners of websites that allow you to enter payment details should always use verified certificates hosted from the most famous certification authorities. Thanks to this, they minimize the risk of the certificate failure affecting their business activities.

LE certificates are anonymous and despite the fact that they provide encryption, they do not solve the problem of anonymity on the Internet. In the event of high competition in a given sector, every opportunity to stand out should be used, including the use of a certificate confirming the organization's data.

Summary

OV and EV certificates are one of the possibilities of building a coherent and digital identity of 21st century websites

- 1 Users should be able to easily identify with whom they are transacting
- 2 EV is still recognizable and used as best practice for identity verification
- 3 Legitimate organizations still want their identity to be clearly visible to users
- 4 Free certificates do not answer all problems related to securing a website and are prone to irregularities


The power of creation.

www.assecods.pl

ASSECO
DATA SYSTEMS

Legal reservations

The content of the presentation is proprietary and protected by law. Texts, graphics, photographs, sound, animations and films, as well as the manner of their arrangement in the presentation, are protected under the applicable provisions, in particular the Act on Copyright and Related Rights and the Act - Industrial Property Law. Any unauthorized use of any content contained in the presentation may violate the rights of Asseco Data Systems S.A. (proprietary copyrights, protection rights to trademarks or other) or rights of Asseco Poland S.A. to the extent that Asseco Data Systems S.A. uses the content to which Asseco Poland S.A. is entitled on the basis of concluded contracts and agreements. The content available in the presentation may not be modified, duplicated, publicly presented, performed, distributed or used for other public or commercial purposes, unless Asseco Data Systems S.A. will give its express consent in writing. Copying for commercial purposes, disseminating, modifying or adopting the content of this presentation (in whole or in part) by third parties is not permitted. Asseco Data Systems S.A. stipulates that the presentation may contain content that refers to offers and services of third parties. The terms of using the offers and services of third parties are determined by these entities.

Asseco Data Systems S.A. bears no responsibility for the conditions and consequences of using the offers and services of these entities. The data and information contained in the presentation are for general information purposes only. The presentation was prepared based on and using Inscale products. The Inscale logo, which includes the word "inscale" in a bold, lowercase font and the tagline "preparation for business" in a smaller font below it.

Name and logo of Asseco Data Systems S.A. and Asseco Poland S.A. are registered trademarks. The use of these marks requires the express consent of the above-mentioned entities.

2020 © Asseco Data Systems S.A.