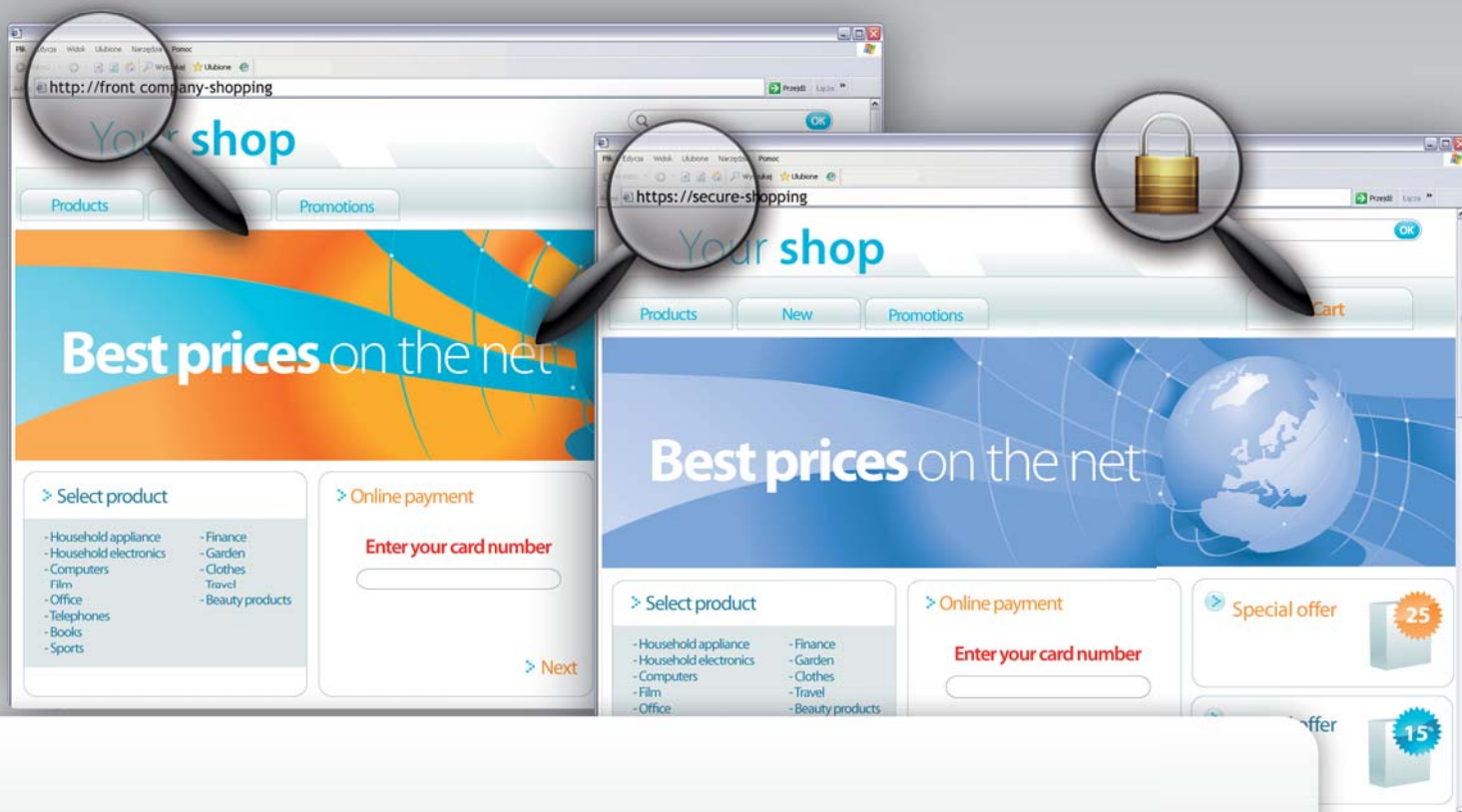


# Which of them is more secure?

Pay attention to details



## SSL Certificates

RELIABILITY OF WEBSITES  
AND SECURITY OF DATA TRANSFERS

SSL protocol provides security for PKI communications by authenticating a server to ensure reliability of its related website. It guarantees reliability of particular websites and servers and ensures confidence of electronic data transfers. The history of SSL goes back to 1994 when Netscape developed a Secure Socket Layer Protocol for secure transmission of encrypted data streams. In the following years SSL technology was further developed by the Transport Layer Security (TLS) working group appointed by the Internet Engineering Task Force (IETF), who published their proposed standard in January 1999.

### Examples of SSL applications

Owing to their high functionality and relatively low costs SSL protocols are widely applied in the following areas:

- Website services:
  - online shops;
  - online banking;
  - electronic public administration: e-offices, electronic registry boxes, public information newsletters;
  - personal data collection and processing services, e.g. those using visitor registration forms (hotels, social utilities, Internet forums, health service establishments, etc);
  - online payment services,
  - online school services providing access to student information, school reports, etc;
  - online log-in services to enable management of e-mail boxes, domains or servers.

### Other SSL applications

- secure file transfer protocol (SFTP);
- network routing;
- Microsoft Exchange incoming (POP3, IMAP) and outgoing (SMTP) mail servers (Outlook Web Access, ActiveSync, Outlook Anywhere, Autodiscover);
- database communications, if not supported by secure local networks or VPN;
- protection of communications between dispersed systems and databases;
- protection of client/server communications.

### Benefits of SSL certificates

**Reliability**

SSL certificates authenticate servers and websites and their assigned Internet domains. By clicking a lock entry, a user is able to check for the host of a selected server or website.

**Data security**

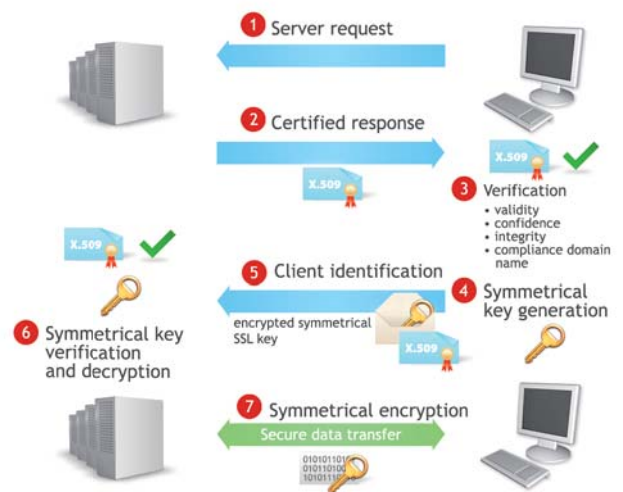
Encryption of communications between a protected server and a user's browser ensures confidence of transferred data and prevents information from being intercepted and used by third parties.

**Protection of personal rights**

SSL certificate provides protection against fraudulent actions of third parties both for owners and users of a server or website.

**Confidence and image building**

SSL-protected server or website proves its owner's responsible approach to the issue of Internet security. By protecting their clients' personal data, service providers improve their market image while raising clients' confidence.



Simplified schema of encrypted communication with SSL protocol

### WebTrust<sup>SM/TM</sup>

The WebTrust<sup>SM/TM</sup> certification seal is a proof of CERTUM - General Certification Authority compliance with international standards of information security services. WebTrust<sup>SM/TM</sup> is a set of necessary good practice procedures for operators active in the area of information security. The WebTrust<sup>SM/TM</sup> certification seal placed on your website is the assurance of its compliance with specific Internet security standards, confidence of data, and reliability of online communications and e-commerce.

The WebTrust<sup>SM/TM</sup> certification ensures high security status for your clients' online transactions. CERTUM - General Certification Authority certificates are the only ones in Poland to be globally trusted, e.g. by all world's most popular Internet browsers and all Microsoft products.



RECOMMENDED

	TRUSTED SSL	WILDCARD DOMAIN	ENTERPRISE SSL	COMMERCIAL SSL	International competitors
Features	• Highest confidence and security	• Multiple sub-domain support • Minimum formalities	• High verification level • Minimum formalities	• Simple and fast delivery • Minimum formalities	Varied across products
Period of validity	7 years	1 year	1 year	1 year	from 1 to 2 years
Level of security and reliability					Varied across products
Financial guarantee	250 000 \$	100 000 \$	100 000 \$	10 000 \$	Up 2 000 \$ to 250 000 \$
Data encryption	to 256 bit	to 256 bit	to 256 bit	to 256 bit	40 - 256 bit
Standard time of delivery	24h	24h	24h	24h	immediately or within 7 working days
Recommended key length	2048 / 4096	2048 / 4096	2048 / 4096	2048 / 4096	512 - 4098
SHA algorithm	SHA-1	SHA-1	SHA-1	SHA-1	MD-5, SHA-1
Free CERTUM SSL seal					Free and commercial versions available
Server Gated Cryptography (SGC)	✓	✓	✓	✓	✓
Free multi-server licence	✓	✓	✓	✓	✗
Activation Card	✓	✓	✓	✓	✗
Support of most popular browsers	✓	✓	✓	✓	✓
Free revocation and replacement	✓	✓	✓	✓	✓
Multiple sub-domain protection under single domain	✗	✓	✗	✗	Varied across products
Assigned client details	• Name of organisation • Name of domain	• Name of organisation • Name of domain	• Name of organisation • Name of domain	• Name of domain	Varied across products
Recognised as trusted authority by most popular Internet browsers	<ul style="list-style-type: none"> <li>• Internet Explorer 5.x +, • Mozilla Firefox 0.9x +, • Mozilla Thunderbird 0.9x, • Opera9.5 +,</li> <li>• Red Hat Linux Konqueror (KDE), • Google Chrome 1.01+, • Seamonkey 1.1+, • AOL 5+,</li> <li>• Netscape Communicator, • Apple Safari</li> </ul>				Varied across products

For more information dial:  
+48 91 4801 340 or go to: [www.certum.eu](http://www.certum.eu)

SSL trusted certificates provided by CERTUM CA ensure protection for servers and websites operated among others by:

- Cooperative banks
- CERTUM CERTIFICATION AUTHORITY
- Polish Ministry of Education
- Polish Ministry of Economy
- Civil Legislative Initiative
- PGNiG (gas exploration and production company)



## Unizeto Technologies SA

Unizeto Technologies SA, operating since 1965, is counted among the local and global leaders of IT industry as:

- qualified provider of electronic signature certification services;
- provider of high-tech outsourcing services;
- developer and integrator of Public Key Infrastructure (PKI) solutions;
- authorised and accredited IT Training Centre.

The products and services offered by Unizeto Technologies SA are based on original solutions and patents developed through R&D projects carried out in cooperation with recognised scientific centres. Unizeto Technologies SA is also a coorganiser of the European Forum on Electronic Signature ([www.efpe.eu](http://www.efpe.eu)), an annual international conference held since 2001 to discuss the theory and practice in the general usage of an electronic signature in business and public administration.

## Authorisations received

- WebTrust<sup>SM/TM</sup> compliance audit qualifying CERTUM General Certification Authority as one of the main certification authorities trusted by Microsoft products;
- ISO 9001:2008 quality management compliance certificate;
- Entry no. 1 in the register for qualified providers of electronic signature certification services;
- Concession no. B-082/2004 granted by the Minister of Internal Affairs and Administration for development and marketing of products and technologies of military and police application;
- Registration in the telecommunication company register made by the President of the Office of Telecommunication and Post Regulation;
- AQAP 2110:2009 compliance certificate - supplementing and expanding the ISO 9000 standards by requirements specific to deliveries of military-purpose goods;
- PN-I-07799-2:2005 compliance certificate in respect to technical and human resource capabilities and satisfaction of legal information security requirements in the areas of design, development and implementation of IT systems, electronic signature certification services and Data Centre services;
- Decision no. 4/014497/06 issued by the Ministry of Economy on expanding the scope of electronic signature services provided by Unizeto Technologies SA.

## CERTUM General Certification Authority



Established in 1998, CERTUM is a Certification Authority based on Unizeto Technologies' self developed proCertum software abroad, with a large selection of PKI certification services. CERTUM - General Certification Authority caters for the needs of public sector institutions, wide range of businesses and individual clients with services including:

- issuance and management of qualified and non-qualified certificates;
- issuance and management of SSL certificates;
- verification of online certificate status protocols (OCSP);
- data validation and certification (DVCS);
- delivery authority;
- security-related audits and consultation;
- training authorised by the Internal Security Agency;
- Electronic Registry Box (ERB) services;
- reliable time stamping.

## Data Centre

One of the most advanced IT outsourcing centres with human and technical resources suited to provide the following services:

- secure electronic archiving;
- Electronic Registry Box (ERB) services;
- e-administration;
- digitalisation and scanning of documents;
- data processing;
- application service provision (ASP);
- data backup and archiving;
- administration of e-invoicing systems;
- hosting and collocation;
- maintenance of contingency data centres;
- mass correspondence servicing - printouts and enveloping;
- WebNotarius® - verification of various certificates and electronic signatures.



Product information: +48 91 4801 340  
[info@unizeto.eu](mailto:info@unizeto.eu)

Unizeto Technologies SA  
ul. Królowej Korony Polskiej 21, 70-486 Szczecin, Poland  
tel. +48 91 4801 201, fax +48 91 4801 220  
[www.unizeto.eu](http://www.unizeto.eu)

Data Centre:  
ul. Bajeczna 13, 71-838 Szczecin, Poland

### Branch offices:

02-078 Warszawa  
ul. L. Krzywickiego 34  
Poland

20-718 Lublin  
al. Kraśnicka 31  
Poland

40-142 Katowice  
ul. Modelarska 12  
Poland

75-212 Koszalin  
ul. Morska 35  
Poland

