

CODE SIGNING CERTIFICATES

BE RELIABLE!

Learn about Code Signing Certificates

Thanks to Code Signing Certificates, developers can electronically sign their software and make it reliable in the eyes of users. Customers, when starting an application under a given operating system, receive friendly messages informing about software recognition.

How does it work?

It is possible that a signed software code is resistant to unnoticeable changes introduced by third parties and viruses, and the certificate used in the code signing process contains publisher data entered by a trusted Certification Centre.

Choose your certificate!

Certificate for Microsoft Authenticode

If you want your software, developed for MS Windows operating systems, to be credible for its users, then code signing with Microsoft Authenticode Certificate would be very useful in your work.

When starting an application, customers receive friendly messages informing about software recognition. Therefore, they are sure that the applications they use are authentic and the certificates used for the purpose of their signing are compatible with MS Windows operating systems. Users are informed that a given application comes from a known and reliable source - the certificate proves identity of the software developer by providing the name of the author or the company, which created the application.

The certificate conforms with the Microsoft Authenticode technology.

Application

Signing of the following:

- Windows operating system libraries,
- ActiveX components and controls,
- binary files (.exe).

Software Publisher

Signing the code of the software you have developed with the Software Publisher certificate makes the software user-friendly.

Thanks to the data on the publisher included in the certificate (name of the application author, information on the company), the user is sure to be using software from a reliable source. Everyone wishing to sign their software code for most of the popular operating systems will surely benefit from the certificate.

Application

Signing of the following:

- Firefox and Netscape extensions,
- UNIX/Linux software,
- VBA macros,
- Apple applications (MacOS X),
- Adobe AIR.

Java Code Signing

Code signing with the Java Code Signing certificate makes the signed software developed for the Java environment trustworthy. When starting an application, users are informed that the application comes from a known publisher. A friendly message will include details on the software developer.

The certificate is compatible with and is recognised as trusted in the Java environment.

Application

Signing of the following:

- Java applets,
- Java-based Internet applications.

3 main advantages resulting from software code signing

Reliability

Users are informed that the application comes from a reliable and trusted source. The certificate provides information on the author and/or the company, which developed the software. Otherwise, users are informed that the file is not signed, or that it cannot be verified and may be harmful to their computers.

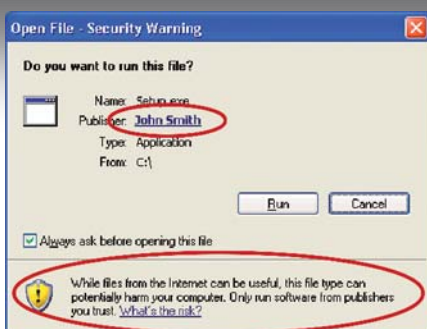
Security guarantee

Proper e-signature verification of software to be installed ensures the user that software has not been modified by third parties (e.g. hackers) or viruses.

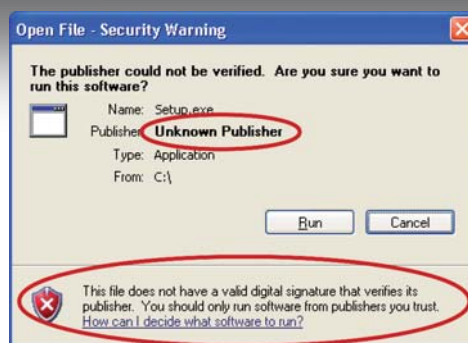
Trust

Code signing means no more messages on “unknown publisher” or “harmful software” in the case of Microsoft and Java operating systems, which appear in the case of applications without an electronic signature.

Microsoft Authenticode messages



A friendly message on recognition of the software source



A warning message displayed in the case of an unknown software source

Features of code signing certificates

Information	Name	Microsoft Authenticode	Java Code Signing	Software Publisher
GENERAL	Features			
	Application	Signing of the following: <ul style="list-style-type: none"> ActiveX components and controls binary files (.exe) 	Signing of the following: <ul style="list-style-type: none"> Java applets Java-based Internet applications 	Signing of the following: <ul style="list-style-type: none"> Firefox and Netscape extensions UNIX/Linux software VBA macros Apple applications (MacOS X) Adobe AIR
	Financial guarantee	10 000 \$	10 000 \$	10 000 \$
	Validity period	1 year	1 year	1 year
	Standard issue time from data verification	24h	24h	24h
	Entity verification level	<ul style="list-style-type: none"> Confirmation of the liability for the certification process Official document to verify company/institution authenticity 	<ul style="list-style-type: none"> Confirmation of the liability for the certification process Official document to verify company/institution authenticity 	<ul style="list-style-type: none"> Confirmation of the liability for the certification process Official document to verify company/institution authenticity
	Required documents for the purpose of identity verification	<ul style="list-style-type: none"> Natural persons: a signed or notarised copy of the ID card of the subscriber Organisations or legal entities: a signed or notarised copy of the ID card of the person responsible for the certification process 	<ul style="list-style-type: none"> Natural persons: a signed or notarised copy of the ID card of the subscriber Organisations or legal entities: a signed or notarised copy of the ID card of the person responsible for the certification process 	<ul style="list-style-type: none"> Natural persons: a signed or notarised copy of the ID card of the subscriber Organisations or legal entities: a signed or notarised copy of the ID card of the person responsible for the certification process
	Documentation and customer service in Polish	✓	✓	✓
	Cancellation and replacement free of charge	✓	✓	✓
	Recording a certificate on a cryptographic card	✓	✓	✓
Time stamping free of charge	✓	✓	✓	
TECHNICAL	Recommended key length	2048 / 4096	2048 / 4096	2048 / 4096
	Hash algorithm	SHA-1	SHA-1	SHA-1
	Exemplary supported formats ¹	.exe, .dll, .ocx, .cab, .msi, .msp	.jar, .war, .ear	.docm, .xlsm, .pptm, .xpi
	Exemplary signing tools	<ul style="list-style-type: none"> SignTool SignCode Visual Studio Express 	<ul style="list-style-type: none"> Jarsigner and verifier with Java JDK 1.5+ 	<ul style="list-style-type: none"> MS Office 2000+ ToolSign.sh and openssl for UNIX/Linux Firefox, Key Manager
	Technical requirements for downloading the certificate	<ul style="list-style-type: none"> Microsoft Internet Explorer 5.0 or higher MS Windows 2000, XP, Vista (32 bit), Windows 7 (32 bit) 	<ul style="list-style-type: none"> Internet browser supporting X.509 v.3 certificates (e.g. Internet Explorer, Opera, Firefox) MS Windows 2000, XP, Vista (32 bit), Windows 7 (32 bit), Linux/UNIX Java JDK 1.5+ 	<ul style="list-style-type: none"> Internet browser supporting X.509 v.3 certificates (e.g. Internet Explorer, Opera, Firefox) MS Windows 2000, XP, Vista (32 bit), Windows 7 (32 bit), Linux/UNIX
	Recognised as trusted by the most common internet browsers, operating systems and applications	<ul style="list-style-type: none"> Microsoft Internet Explorer (IE) 5+, Mozilla Firefox 0.9+, Opera 9.5+, Google Chrome 1.01+, Apple Safari 4.0, AOL 5+, Netscape Communicator 4.51+, Camino Konqueror (KDE), Apple iPhone, iPod, Safari 3.0, Opera Mini 4.10+, Microsoft Windows, Apple MacOS X (10.5.8+), Linux (OpenSSL v0.9.5+), Microsoft Outlook 2003, Mozilla Thunderbird 1.0+, Netscape Communicator 4.51+, Apple Mail, The Bat, Microsoft Office (Word, Excel, Powerpoint, Access, InfoPath), Mozilla Suite v.0.9.9+, SeaMonkey, Microsoft Authenticodes & Visual Basic Applications (VBA), Sun Java JRE (1.4.2 Update 16+, 5.0 Update 13+, 6 Update 3+) 		

1 - and other types of files supporting e-signature

Java Code Signing messages



A friendly message on recognition of the software source



A warning message displayed in the case of an unknown software source

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), 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^{SM/™} 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

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

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



● Registration points

● Identity verification points

www.certum.eu