CertiID SSL certificates

Help build trust and secure your website for e-commerce or confidential communications

Nowadays, the Internet is a vital part of any business organization. With confidential data increasingly being transferred over the Internet, companies are aware of the need for absolute security and confidentiality. However, extensive reports of fraud attempts, phishing attacks and cybercrime in general, have made customers hesitant to share personal or financial details online. Fraudsters frequently impersonate legitimate businesses luring visitors into divulging personal information.

CertiID SSL certificates overcome these credibility issues and add trust to online transactions. They provide website authentication and ensure customers, employees or partners that their information remains secure in transit. CertiD SSL certificates are indispensable for organizations that exchange sensitive personal and financial information, credit card or login credentials online!

SECURE SOCKET LAYER TECHNOLOGY FOR IDENTITY ASSURANCE

CertiID SSL certificates work with Secure Socket Layer technology. It is an industry standard which is used to establish an encrypted connection between a web server and an internet browser. This encryption prevents sensitive data such as personal credentials or credit card details from being intercepted during transmission. All data exchanged between web server and web browser will be secured. CertiID SSL certificates are easy to use and offer a reliable identification of your website and organization.

An CertiID SSL certificate performs three security services:

1. Confidentiality: information cannot be intercepted
2. Authentication: is the company the legitimate owner of the company's website?
3. Integrity: the communication cannot be altered in transit without detection

VASCO Data Security offers two types of SSL certificates: a standard SSL certificate for organization validation and an EV SSL certificate for extended validation.

STANDARD CERTIID SSL CERTIFICATES FOR ORGANIZATION VALIDATION

A standard CertiID SSL certificate provides website authentication and verifies domain name ownership and the company. Websites that have an SSL certificate can be recognized by the padlock icon in the browser and the https prefix in the URL. Incorporating an SSL certificate ensures visitors of your website that your website is secure and all information will be encrypted.

CERTIID EV SSL CERTIFICATION FOR EXTENDED VALIDATION

CertiID EV SSL certificates are commonly used to secure e-commerce sites and assure customers that your website is trustworthy and they can interact online with confidence. CertiID EV SSL certificates are recognizable by the padlock icon in the browser and the display of the name of the CA – for CertiID certificates the CA is DigiNotar - which has issued the certificate. The green bar ensures that the legitimacy of the business has been validated by a third party and that the website belongs to that company and not that of an imposter.

EV SSL certificates set a new standard for SSL certificates and introduce a standard trust level that is implemented by Certificate Authorities (CA) worldwide. CertiID EV SSL certificates are issued according to a specific set of identification verification criteria. Those criteria are verified by a Certification Authority before the certificate is issued. The requesting company must meet the Extended Validation Guidelines established by the CA. The identification process confirms domain name ownership and includes an authentication process, verification of the business by government or third party business registries.

BENEFITS FOR YOUR ORGANIZATION

- More confidence attracts more visitors
- Competitive advantage thanks to added trustworthiness
- Protect customer accounts from phishing attacks
- Secure exchange of sensitive information
- Protect your brand from copycat websites

ONLINE MANAGED CERTIFICATES

Should your organization require a large number of CertiID (EV) SSL certificates, you can use the online CertiID managed SSL portal which enables you to manage your own certificates. Your organization carries the responsibility for the accuracy of the information in the certificates.

TECHNICAL DETAILS

	Standard CertiID SSL certificate	Extended Validation CertiID SSL certificate
Validity	4 years	2 years and 3 months
Root chain	DigiNotar Root CA DigiNotar Root CA	DigiNotar Root CA DigiNotar Extended Validation CA
Insured amount	€ 500,000	€ 500,000
Reliability	High reliability	Optimum reliability according to CAB forum guidelines
Security visibility	Clickable padlock icon	Green URL bar Clickable padlock icon Display of CA that issued certificate
Automatically trusted Internet browsers	Internet Explorer from version 7 and up Safari iPhone from version 10.5.7 Chrome Firefox from version 3 Opera from version 9.64	Internet Explorer from version 7 and up Safari iPhone from version 10.5.7 Chrome Firefox from version 3 Opera from version 9.64
Key length	Standard 2048 bits 4096 bits also available	Standard 2048 bits 4096 bits also available
Encryption	Minimum 160 bit	Minimum 160 bit
Data Certificate	CN = FQDN Serial number = DigiNotar serial number OU = department (optional) OU = SSL Servercertificate – See CPS L = Place Address number (Branche number) O = Organization name (Chamber of commerce number or other unique number) C = Country code RFC-822: Email address (optional)	CN = FQDN Serial number = Chamber of Commerce number or other unique number OU = Department (optional) OU = Extended Validation SSL Certificate - See CPS L = Place Address number (Branche number) O = Organization name (Chamber of commerce number or other unique number) C = Country code 1.3.6.1.4.1.311.60.2.1.1 = Place 1.3.6.1.4.1.311.60.2.1.3 = Country code 2.5.4.15 = type business category

About VASCO

VASCO designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXs GUARD® authentication products for the financial world, remote access, e-business and e-commerce.
With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

www.vasco.com

BRUSSELS (Europe)
phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (North America)
phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)
phone: +61.2.8061.3700
email: info-australia@vasco.com

SINGAPORE (Asia)
phone: +65.6323.0906
email: info-asia@vasco.com

DS-201106-v1