

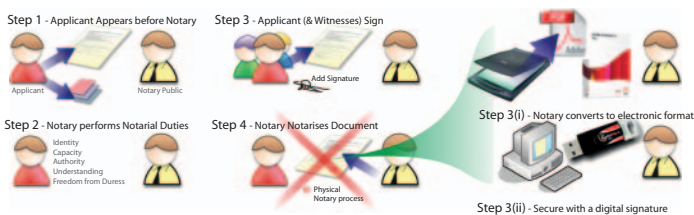
Best Practice Guidelines for Governments

eApostilles & eRegisters with Certified Document Services (CDS) and ExtendedSSL

Where to put the 'e' in eNotarisation?

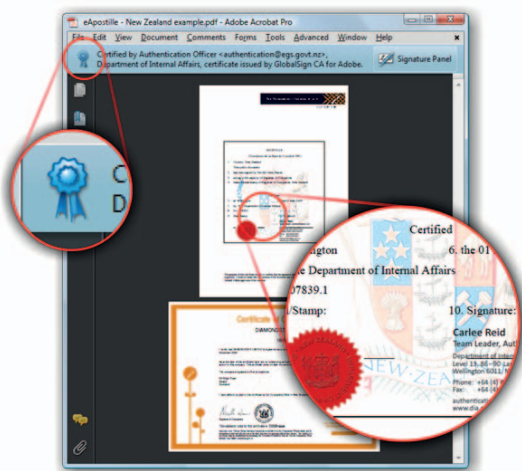
Digital certificates are required to create digital signatures (cryptographically strong electronic signatures) on e-documents. Until such time as applicants and witnesses are able to present valid digital IDs and until such time as documents are provided in a purely electronic format, wet ink signatures should continue to be used in exactly the same way as they are today (1-3 below). The 'e' in eNotarisation is introduced by simply replacing the final step (4) in the traditional Notary process, with two very simple processes; Firstly, converting (i.e. scanning) the final document to an internationally accepted electronic format (3(i)) such as PDF and digitally certifying the resulting content (3(ii)).

The digital certificate used by the Notary to certify (i.e. Notarise) the PDF is provided by a Certification Authority (CA) via a RA (Registration Authority) and is delivered and controlled under a strict Certificate Policy. In this respect, the authenticity of the signature can be verified automatically by some 800+ Million copies of Adobe's PDF reader in use around the world. This simple fact removes the myriad of issues created when individual countries, organisations and individuals try to control individual trust models across international boundaries where the recipient's software cannot be guaranteed.



The process to support eApostilles

Competent bodies can now receive eNotarised public documents from Notaries, automatically validate the electronic signature is authentic and at the same time be assured that the Notary is legitimately practising as a notary (The Registration Authority has the capability to revoke a Notary's certificate). The Notary simply needs to insert an electronic Apostille (eApostille) 'blank form' into their document prior to submission. It is this form which is then signed by the competent body. Competent bodies may also add an electronic eApostille to electronic versions of public documents created by other trusted government bodies.

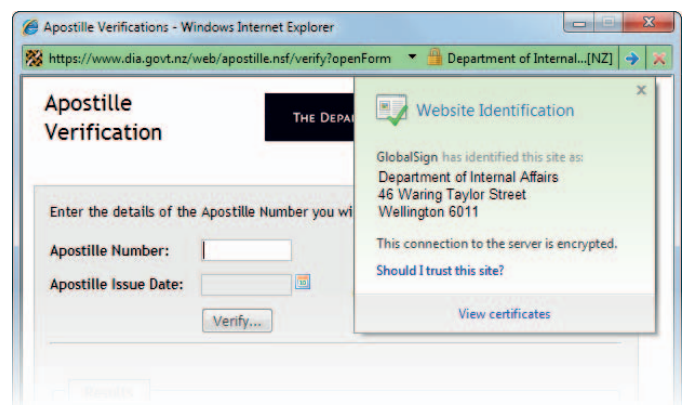


For more information about GlobalSign solutions, please call UK +44 1622 766 766 or Belgium +32 16 89 19 00

Visit www.globalsign.co.uk or www.globalsign.eu for more information

Why and how to protect your eRegister

Relying parties who are NOT able to look at the electronic version of the digitally signed PDF (i.e. a document which may have been printed out), must be able to verify the authenticity of the Apostille via the Apostille register. Although the integrity of the print out is not possible to check via this method, the relying party can be assured of the legitimacy of the Apostille and the authenticity of the website of the competent body. This avoids the possibility of an attacker assuming the identity of the competent body via a fraudulent website and offering false guidance.



SSL Certificates, the security technology that activates the yellow padlock, is essential for all websites conducting ecommerce or capturing customer data or wishing to present authentic data to relying parties. As you are probably aware, there have been recent advancements in how SSL can be used which aid the level of identity assurance provided. Called Extended Validation SSL (EV SSL), it represents the most significant advancement in how customers see and understand the authenticity of the information they see via their internet browsers. The latest group of browsers show a green address bar to highlight the added authenticity of the website. Relying parties are also able to 'click' on the padlock for additional information as shown in the screen capture above of an IE7 browser session utilising this technology.

Customer Case Study



An eApostille example in operation

New Zealand was the first authority to roll out a service based upon CDS digital certificates. This milestone was announced and recorded by the HCCH via the following link on the HCCH site.

http://www.hcch.net/index_en.php?act=events.details&year=2009&varevent=167
As this example opposite shows, the authenticity and integrity of documents which are signed by the competent body in New Zealand are now available to 800 million people worldwide in multiple languages. Best practice for the format of the electronic Apostille (e-App) document was taken from the HCCH/NNA web site providing guidance to competent bodies (<http://www.e-app.info>)

Next steps for New Zealand's Apostille register

The authentication unit within the Department of Internal Affairs now also offers an Apostille register allowing relying parties to check the authenticity of the Apostille reference number contained within the Apostille PDF documents that are printed out. From Q3 2010 the eRegister has been secured with an ExtendedSSL certificate to provide assurance to relying parties to validate the source of the register.

PDF Signing for Adobe CDS - How it Works & Solutions by Industry

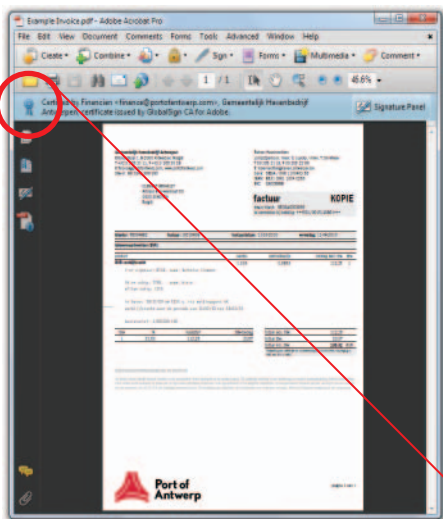
Certified Document Services (CDS) provides a cost effective PDF digital signing solution.

How it Works...

Certified Document Services (CDS) is a service which is enabled by the Adobe root certificate authority and was introduced into the Adobe® Acrobat® product range supporting SHA-256 signatures from version 7.0 onwards. CDS empowers document authors to digitally sign Portable Document Format (PDF) files, using an industry standard X.509 digital certificates chained to the Adobe Root Authority to allow automatic validation of authenticity of the author using the free Adobe Reader software. No additional client software or configuration is required.

A major advantage to any organisation with stakeholders in multiple countries, is the built-in international language support within the PDF reader itself. Available in over 30+ languages, Adobe Reader ensures a consistent digital signature experience worldwide. CDS was designed specifically to enable any organisation providing documents to large and disparate recipients, who may be in multiple countries, to increase the assurance level of the document. The document's integrity and authenticity are digitally preserved by the addition of the CDS signature to the PDF. Document authors are able to increase this assurance level without requiring recipients to deploy additional processes - it simply works, ensuring an effective ROI through a vast reduction in the investment normally associated with supporting a proprietary security system.

Following a thorough verification of the 'Applicant' requesting a PDF Signing for Adobe CDS certificate, GlobalSign will issue a 'pickup' link which allows a certificate to be generated and securely stored on a SafeNet® hardware cryptographic device. Authors can digitally certify PDFs using certificates "chained" up to the trusted Adobe Root. Recipients simply need to open the document using the Adobe free reader to instantly verify the authenticity and integrity of the document. Adobe's simple to interpret "Blue Ribbon, Yellow Warning Triangle, and Red X" trust messaging allows even novice users an easy to understand method to determine if the document is legitimate.



Valid and certified!
Authenticity and Integrity are verified
Pass



Error!
Authenticity Check Fails



Error!
Integrity Check Fails

For more information about GlobalSign solutions, please call UK +44 1622 766 766 or Belgium +32 16 89 19 00

Visit www.globalsign.co.uk or www.globalsign.eu for more information

Solutions by Industry

Electronic Invoicing

Electronic VAT invoicing offers numerous advantages to organisations both large and small – cost reductions, low carbon footprint ecosystems, greater security and trust for all stakeholders and faster cash collection than traditional out-dated paper billing.

<http://www.globalsign.co.uk/solutions/industry-solutions/e-invoicing.html>

Healthcare

The New England Journal of Medicine, 2004, reports "paperwork represent 31% of all healthcare costs". CDS can help relieve the burden on physicians surrounding cumbersome processes involving patient paper-work while being part of a CFR 21 Part 11 compliant solution.

<http://www.globalsign.co.uk/solutions/industry-solutions/healthcare.html>

Manufacture and Design

Architecture, Engineers and Construction (AEC) professionals benefit from CDS with faster design collaboration, more efficient and less expensive electronic document storage, and stronger protection via tamper evident engineering and product documentation as documents are exchanged among customers, partners, contractors, and building departments.

<http://www.globalsign.co.uk/solutions/industry-solutions/manufacturing.html>

Education

More and more educational institutions are increasing student and alumni satisfaction as universities and colleges disseminate sensitive documents like transcripts and admissions letters electronically in a fraction of the time and costs seen with their paper equivalent.

<http://www.globalsign.co.uk/solutions/industry-solutions/education.html>

Government

CDS supports both local and federal government initiatives including the Government Paperwork Elimination Act helping reduce costs, enhance citizen accessibility to government information and reduce unnecessary environmental waste while at the same time providing high assurances to its citizens that the information is legitimate.

<http://www.globalsign.co.uk/solutions/industry-solutions/government.html>

Financial Services

Industry best practices coupled with government imposed regulation like Sarbanes-Oxley make CDS an attractive option as a thorough audit of the signature properties are embedded in the document itself. Well after the Digital ID expires, the signature characteristics are preserved providing relying parties strong authentication of both the organisation and individual or role that signed the PDF, whether the content is still intact, and the exact date and time of the transaction as determined by a RFC 3161 compliant time-stamp.

<http://www.globalsign.co.uk/solutions/industry-solutions/financial-services.html>

The Notarial and Legal Professions

CDS provides unequalled support of trusted documents in multiple languages. This alone facilitates cross border transactions as both sides are able to interrogate the authenticity of a document in their local language; the ideal solution for e-Notarisation.

<http://www.globalsign.co.uk/solutions/industry-solutions/notary-legal.html>

The SafeNet iKey 4000 & 5100

GlobalSign's PDF Signing for Adobe CDS Certificates are usually provided with either a SafeNet iKey 4000 (SHA1 capable) or a SafeNet iKey 5100 (SHA256 capable). As an extension of smart card technology both keys plug into any USB port to provide strong portable user authentication without the need for costly reader devices. Certificates installed on to either token ensure regulatory compliance with the FIPS 140-2 Level 2 requirements of the Adobe CDS program.

For organisations with high volume signing requirements or the need for automation, GlobalSign is able to provide a HSM (Hardware Security Module) in either PCI, PCI(e) or Network attached.

In addition, GlobalSign's ePKI (Enterprise PKI) solution is available for companies that require multiple digital identities.

