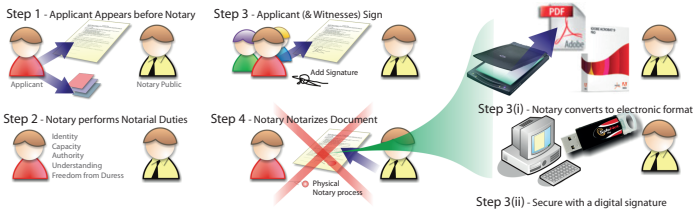
Best Practice Guidelines for Governments

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

Where to put the 'e' in eNotarization?

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 eNotarization 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. Notarize) 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, organizations and individuals try to control individual trust models across international boundaries where the recipient's software cannot be guaranteed.



The process to support eApostilles

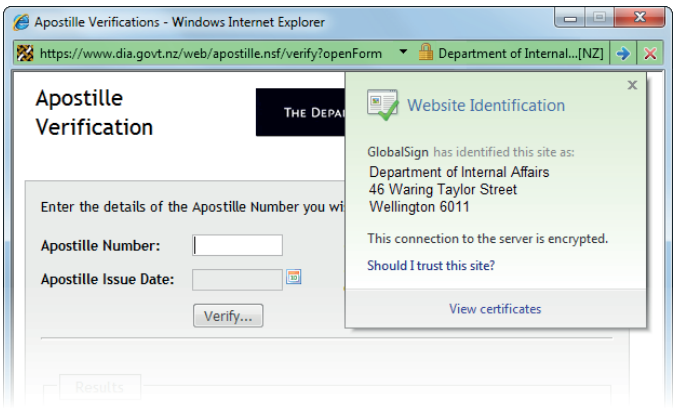
Competent bodies can now receive eNotarized public documents from Notaries, automatically validate the electronic signature is authentic and at the same time be assured that the Notary is legitimately practising as a notary (The Registration Authority has the capability to revoke a Notary's certificate). The Notary simple 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 603-570-7060 or 877-775-4562

Visit www.globalsign.com 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 utilizing this technology.

Customer Case Study

THE DEPARTMENT OF INTERNAL AFFAIRS
Te Tari Taiwhenua

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.