The Application of HSM Technology in Electronic Invoicing

The Servicio de Administración Tributaria (SAT), Mexico’s tax authority, in 2011 began requiring applicable businesses to convert all invoices to an electronic format in an effort to reduce cost, standardize procedures, and deter fraud. In order to assist organizations in complying with these regulations, Mis e-Folios turned to Futurex to provide a secure, compliant, hardware-based electronic invoice authentication solution.

Electronic invoicing is a technology which is quickly evolving around the world to become a method for streamlining administrative processes, providing instantaneous validation, and ensuring the authenticity of identities.

Beginning January 1, 2012, the Servicio de Administración Tributaria (SAT), Mexico’s tax authority, made it compulsory for certain organizations filing taxes in Mexico to digitize business invoices and receipts. These regulations require businesses to standardize with the SAT, sending and storing invoices electronically in a compliant format that has been authenticated using a hardware-based platform.

Under the new rules, Mexican companies must utilize third-party organizations with an Authorized Provider Certification (PAC) approved by the SAT to file their Digital Tax Receipts via the Internet (CFDI), which should include their Electronic Signature Certificate (FIEL) and the Electronic Seal Certificate (CSD). As these regulations are still evolving, in 2014, organizations taking in gross revenue exceeding $220,000 MXN per year will be required to comply with these regulations.

The PAC utilizes a hardware security module to issue a digital signature on their client’s invoice. This digital tax receipt documents and confirms that a business transaction is in accordance with the standards defined by the SAT and is generated, transmitted, and protected by electronic means. Further, these invoices must be stored digitally to be able to refer back to them in case any clarification is required.

Electronic invoicing relies on a Public Key Infrastructure (PKI) to generate a digital signature, a process commonly referred to as digitally signing a document. This certification process ensures the authenticity and integrity of the transmitted data.

About Mis e-Folios

Based in Mexico City, Mis e-Folios is a supplier of high-quality professional services with an Authorized Provider Certification (PAC) verifying their internal processes, technological equipment and the operation thereof by the SAT for issuance, management certifications, and Digital Tax Receipts via the Internet (CFDI). They strive to provide comprehensive and reliable solutions to their customers in an efficient and compliant manner.

http://www.mise-folios.mx
The PAC begins by generating an asymmetric key pair, comprised of a public key and a private key, within its hardware security module using the RSA algorithm. The public key is used along with specific attributes to create a certificate request to be sent to the SAT. The private key is kept secure within the confines of the HSM’s Secure Cryptographic Device.

The SAT, in turn, acting as a trusted certificate authority, uses its private key to sign the PAC’s certificate signing request and generates a certificate, which is composed of identifying attributes and its public key, and sends this certificate along with the parent certificate to the PAC. This ensures that the PAC and the SAT are mutually authenticated entities and that their continued communication is trusted.

Once mutual authentication has occurred, the PAC uses their private key to digitally sign their customer’s financial information stored in an XML-based file format specified in Annex 20 Version 3 of the Mexican Miscellaneous Tax Resolution.

The PAC then uses the SAT’s public key, enclosed in their digital certificate, to encrypt the data. The file is sent through the issuing organization’s firewall to the SAT.

The SAT then uses their private key to decrypt the outer layer of encryption, and the PAC’s public key to verify the PAC’s signature. Once the message is authenticated, the SAT sends the issuer a validating message. This method provides real-time approval of tax documentation and ensures the authenticity and integrity of the message.

The Business Case

Mis e-Folios, as a forward-looking organization, sought to be at the forefront of the developing electronic invoicing standards in Mexico. They contacted Futurex to explore solutions to ensure the integrity and authenticity of their invoices in transit and comply with the Servicio de Administración Tributaria’s new regulations.

Because Mexico’s regulations are new and are still changing, developing a solution that both suited current regulations and evolving regulatory standards was a high priority. Mis e-Folios representatives worked with Sam Telles of the Futurex Solutions Architect team to develop a solution that would fit these new and uncharted regulations.

“We needed a scalable solution that could meet these challenges head-on, and continue to grow and adapt with our company,” Jorge Cordova, IT/Project Manager of Mis e-Folios, said.

After careful analysis and discussion with the Futurex team, Mis e-Folios decided to move forward, selecting Futurex technology to form the core cryptographic infrastructure of their electronic invoicing system.

---

Electronic Invoicing: How does it work?

1. Businesses register with the Servicio de Administración Tributaria, Mexico’s tax authority, to issue electronic invoices and obtain an electronic signature and digital stamp. This information is submitted to an Authorized Certification Provider (PAC).
2. The PAC digitally signs the document and submits it to the Servicio de Administración Tributaria.
3. The Servicio de Administración Tributaria decrypts the message and sends the PAC a validation.
Case Study: The Application of HSM Technology in Electronic Invoicing

The Solution

Working together, the Futurex Solutions Architect team and Mis e-Folios developed a solution that aligned with their business objectives and complied with the technical requirements outlined by the SAT.

“Sam’s knowledge and foresight were invaluable in helping us establish a solution that was not only compliant, but also functional and easy to implement,” Cordova said.

An Excrypt SSP9000 hardware security module was selected, along with RSA support enabled to generate public/private key pairs. The Excrypt SSP9000 has the ability to integrate with Mis e-Folios’s custom API and is RSA-enabled to meet the encryption requirements outlined by the SAT; in particular, that generated keys must be of at least 1024-bit encryption.

Integrated disaster recovery and redundancy features such as dual power supplies and Ethernet ports ensure that Mis e-Folios maintains the 24x7x365 uptime that their customers expect.

Mis e-Folios’ Requirements

Requirement: The SAT requires Authorized Certification Providers to protect private keys within hardware.
The Excrypt SSP9000 is a FIPS 140-2 Level 3-validated Secure Cryptographic Device. All data encryption occurs inside the hardware-based cryptographic module. In the event an attacker attempts to gain access to these keys, the cryptographic module will zeroize.

Requirement: Invoices must be sent to the SAT in an XML-based file format digitally signed by a hardware security module with a public/private key pair
The Excrypt SSP9000 includes RSA support which enables the HSM to generate, verify, encrypt, and decrypt data using PKI.

Requirement: PKI generation must be logged to demonstrate keys were generated inside the HSM
The Excrypt SSP9000 has a syslog feature which can be accessed remotely for auditing purposes.

Requirement: Extensible to accommodate future changes in regulatory requirements
The Excrypt SSP9000 contains a proprietary encryption card designed to function in compliance with the most rigorous standards available.

The Results

Mis e-Folios’ electronic invoicing system was successfully implemented and was certified by the SAT in August of 2012 as an organization authorized to offer digital invoicing services in Mexico. For Mis e-Folios, this means they are able to ensure proper certification, encryption, integrity, traceability, and storage of all electronic invoices in full legal compliance with the SAT’s requirements. Since then, Mis e-Folios has become a leader in providing digital invoicing solutions to its clients.

“Our electronic invoicing solution allowed us to expand our business and increase our service offerings, while continuing to provide our customers with the highest level of security for their sensitive data,” Cordova said.

Because of the successful deployment of Mis e-Folios’ system, Futurex has become one of the Mexican government’s supported hardware vendors and is recommended to all service providers.

“Our electronic invoicing solution allowed us to expand our business and increase our service offerings, while continuing to provide our customers with the highest level of security for their sensitive data,” Cordova said.

Jorge Cordova
IT/Project Manager, Mis e-Folios