Recommendations and Considerations for Bulk Filing Transmission and Security Protocols

presented by

NATIONAL PAYROLL REPORTING CONSORTIUM, INC. (NPRC)

ADP ★ AllianceHCM ★ Apex HCM ★ Asure Software ★ Check
CheckWriters ★ Dayforce ★ Gusto ★ Heartland Payroll Solutions
Intuit ★ isolved ★ Netchex ★ Paychex ★ Paycom ★ Paycor
Paylocity ★ PPI Business Services ★ PrimePay ★ Rippling
Symmetry Software ★ TriNet ★ UKG

January 2024

Table of Contents

Purpose of this Document 3
About the authors of this document 3
Transport Protocol Options 3
Recommendations and Specifications 4
Secure File Transport Protocol (SFTP) 4
Best Practices for SFTP 4
SFTP Technical Specifications 5
Web Services 5
Best Practices for Web Services 6
Web Service Technical Specifications 6
Web Browser Filing Considerations 7
Web Browser Technical Specifications 8
Other Web Browser Considerations 9
Contacting NPRC 10
References 10

Purpose of this Document

Nearly three million U.S. employers, representing more than 48% of the private sector workforce, use a payroll service provider (PSP) to electronically calculate, pay and file employment tax returns. PSPs often assist clients in resolving any problems or errors with such tax filings and payments as part of their payroll service. Generally, PSP interactions with a taxing authority are to send information and tax payments on behalf of clients. The information flow is from the employer to the PSP, and then to the agency. Tax authorities typically only return non-sensitive data, such as confirmation that an electronic file was successfully received.

Due to the increased focus on data security, many taxing authorities are understandably concerned about releasing sensitive data to any potentially unauthorized recipients. PSPs have also increased their focus on data security and align with taxing authorities on the importance of data security. In addition, data and information security is an inherent part of the agreement between employers and their PSPs. However, some states seem to have over-compensated and are now restricting known PSPs from performing high-volume batch operations using automation, and are even rejecting otherwise-valid tax returns due to concerns about security. Some states restrict PSPs' access to file and pay taxes on behalf of their clients if it isn't clear to the state that the PSP is authorized to file and/or pay such taxes. Employers using PSPs often must follow complicated steps to comply with different state requirements to authorize a PSP to file and pay for them.

According to NIST Publication 800-63-3, Digital Identity Guidelines, which provide technical requirements for federal agencies in authenticating of users interacting with government IT systems over open networks, receiving payments and information (such as tax payments and returns) are among the lowest-risk tier, especially if no tax refund is sought. Thus, requiring unique and/or difficult processes to establish authority to pay and file payroll taxes is unnecessary and in fact serves as a barrier to electronic filing.

About the authors of this document

The National Payroll Reporting Consortium (NPRC) is a non-profit trade association whose member organizations provide payroll, tax reporting, tax payment, and related services to more than 1.4 million employers nationwide, covering more than one-third of the private sector workforce. The NPRC actively supports appropriate electronic filing and tax payment programs. In addition to our long-time association and interaction with taxing authorities, we have long worked with the IRS, SSA, and state unemployment insurance agencies to develop and improve standards for electronic filing and related transactions.

Transport Protocol Options

Many PSPs and taxing authorities have experienced decades of excellent performance transmitting data securely through modern bulk filing method options. Below is the list of preferred bulk filing transmission methods, listed in order of preference:

- **Secure File Transport Protocol (SFTP)** is an interactive file transfer program which performs high speed file transfer operations over an encrypted transport. SFTPs generally require very little

initial investment or work to set up the process for either the PSP or the tax authority, and generally require minimal routine maintenance.

- **Web services:** Unattended, point-to-point or application-to-application (A2A) transmission and processing are strongly recommended (e.g., server-to-server capabilities for high-volume filing). Sending XML documents over HTTPS (Web services) is an industry standard for A2A transmissions. This format has been adopted by the IRS Modernized E-file system.

Recommendations and Specifications

The following is intended to outline the specifications needed to support industry standard bulk filing solutions for PSPs.

Secure File Transport Protocol (SFTP)

Secure File Transport Protocol (SFTP) solutions are easy to establish and maintain, and allow for the exchange of large files between known and trusted parties in a relatively brief transmission.

- **Use Cases:** SFTP is preferred by PSPs for tax filings, including amended or corrected returns. SFTP is also commonly used for data validation programs and other exchanges of data between taxing authorities and PSPs.
- **Prevalence of SFTP:** Many government IT offices already have approved SFTP client programs and simply need to expand the usage of the SFTP to include exchange tax filings and other data validation programs with PSPs.
- **State Examples:** Examples of SFTP specifications and guides to aid you in the development of a similar guide for your department include Wisconsin's File Transfer guide and North Dakota's Secure FTP page.
- **Learning More:** For those that are unfamiliar with SFTP, or do not have access to an SFTP client program, there are many ways to run an SFTP communications program, including installing a command line program, a Graphical User Interface (GUI) version of the program, or installing an add-on to a web browser.

Best Practices for SFTP

- Taxing authorities can accept files from trusted or known IP addresses, and conversely block files from unknown IP addresses using accept listing or allow listing practices, or similar security measures. Many states require an annual registration of PSPs' IP addresses in order to ensure that they only receive bulk filings from trusted and vetted partners.
- Tax authorities should not restrict the number of files that can be submitted by a provider each day.
- Tax authorities also should not limit the number of IP addresses that can be registered per PSP. Some states limit the number of IP addresses to two, but large payroll firms often have far more IP addresses that could be used to send a file for redundancy and disaster planning purposes.

SFTP Technical Specifications

- SFTP using SSH (SSH File Transfer Protocol): This protocol supports batch and bulk e-filing, with security being addressed at the SSH2 protocol. Optionally file-level encryption can be supported via use of PGP encryption. This is the safest alternative, with encryption at both the channel and payload levels.
- FTP over SSL channel encryption has the same benefits as above, but security is addressed at the session level by the use of SSL (Secure Socket Layer). Optionally file-level encryption can be supported via use of PGP encryption. This is also a safe alternative, with encryption at both the channel and payload levels.
- FTP with PGP data encryption is easy and widely used, running on virtually every conceivable operating system and platform. Security is addressed at the file level using PGP.
- Third Party Vendor Software supporting TCP/IP over Internet (such as Axway Secure File Transfer, Axway/Cyclone Interchange, Inovis IPNet, SterlingCommerce Connect: Direct – supporting AS1, AS2, AS3 protocol): This is the "Cadillac" version for electronic filing, and can be very costly for agencies and their trading partners. This type of solution will address security/privacy, authentication of sender/receiver, and the integrity of exchanged files is guaranteed with non-repudiation. It is very suitable for high-volume "bulk" electronic filing applications.

Web Services

Web Services should be an additional option for PSPs bulk filing. PSP's serve as conduits to receive tax data from their clients, and in turn generate the tax-related information in bulk file formats and electronically submit the information securely to taxing authorities with their information specified as the Submitter. This service can also support the retrieval of the status of submissions the PSP has transmitted to the taxing authority.

- **Use Cases:** Web services work best for data validations and proactive exchanges between PSPs and tax authorities in order to validate rates, account numbers, deposit schedules, account status, etc.
    - Web services can also be used for tax filings, including amended/corrected returns.
- **Prevalence of Web Services:** Many government IT offices already have approved web services available and simply need to expand the usage to include data exchanges with approved PSPs.
- **Federal & State Examples:** Review the Social Security Administration's EWR Web Service Client Development Reference Guide or California Employment Development Department's bulk filing page as examples in order to create a Web Service client for your department.
- **Learning More:** A good explanation of Web Services can be found here https://rapidapi.com/blog/api-vs-web-service/ for those that are not familiar with some of the terms or related processes. REST [REpresentational State Transfer] is a standardized architectural style that can be used when creating a web API. It is a type of Web Service.

Best Practices for Web Services

a. It is not really necessary to encrypt the "package" in the transmission as the route itself is encrypted, but PGP does provide extra security depending on the tax agency's backend system's behavior for those agencies that desire it.
b. Tax authorities generally cannot provide development support for web service clients, but do provide a development guide, a testing environment, and troubleshooting support.

Web Service Technical Specifications

Application Programming Interface (API)

- The purpose of Application Programming Interface (API) is to document what must be done at the technical level in order to interact successfully with the agency's system.
- The API for Application-to-Application (A2A) transmission documents should be updated at least six months before any changes to the system, and should include a well-defined data format and a secure transmission protocol.
- The A2A transmission protocol should support batched submissions; that is, single transmissions with multiple filings and payments. This is necessary to meet the throughput requirements of large transmitters; the filings and payments may or may not be related to each other.
- The agency should acknowledge the receipt of each batch, or the filings within each batch, in real-time. This does not imply that the agency must accept or reject each tax return in real-time, but it should provide some level of validation of the transmission to ensure authorization, completeness, and proper formatting of the transmission.

Application-to-Application (A2A)

- Web services application-to-application allows employers to communicate with the agency leveraging an industry standard. With this style of interaction, data is exchanged in SOAP messages using the request-response model transport mechanism over an HTTPS connection. Acknowledgements must be retrieved from the same channel that was used to submit the return.
- Web Services typically use a Web Service Definition Language (WSDL) document to specify the API between the communicating applications. Web Services can also be implemented without a WSDL by simply posting an XML document via HTTPS.
- Private sector companies should generally not be asked to install software developed by the agency or an external source. Some arrangements may violate software development control environments. Also, not all software is compatible with industry languages and development tools.
- Adopt industry security standards for Web services such as WS-Security, that allow for well-documented, interoperable, vendor, and tool-supported security implementations. Privacy and confidentiality concerns are paramount in A2A transactions. The IRS MeF system has chosen SAML as a security mechanism.
- Many systems rely on Secure Sockets Layer (SSL) for encryption and server authentication. The manner in which clients are authenticated varies considerably and remains a matter of concern.
    - The PSP needs to have web service client software developed/installed on their machine following the WSDL specification from the agency. The PSP software will send web service requests to the agency web services end-point, and submission data will be attached to the request messages. The PSP software shall also handle the web services responses.

Web services client software is developed by third-party software developers, not the agency system.

- The web service client software should be based on J2EE/.NET or other open source technologies. MIME with MTOM attachment standard is recommended.
- The agency should publish the specifications of the WSDL and the schema of the submission, return, proof of filing or transmission receipt, and the acknowledgements or responses.
- When using the P2P approach, the employer sends a transmission file to the agency. When using the A2A interaction, the employer client application sends a message to the agency.
- A2A is not recommended for the filing of a single return.
- The structure of the web services message used to transmit submissions that use SOAP with attachments is as follows:
    - An e-file transmission file (or eSubmission) is a MIME multi-part document that:
        - Conforms to SOAP 1.1+ with attachments standard
        - Conforms to WS-I Basic Profile 1.1+ standard for interoperability
        - Consists of:
            - A SOAP envelope (also called Transmission Envelope), which contains:
                - A header - the “Transmission Header”
                - A body - the “Transmission Manifest”
            - One or more SOAP attachments
                - Each attachment is a self-contained return, which is one MIME multi-part document (nested within another, the transmission file)
            - MIME boundaries and content headers
        - A return is a MIME multi-part document. A return (within an eSubmission) is a MIME multi-part document and contains XML documents and/or binary attachments:
            - XML Structure
                - The “Return Header” contains information that is common for the whole return
                - The “Return Data” contains all of the XML return documents
                - Binary attachments are non-XML documents

Web Browser Filing Considerations

Browser-based file uploads rely on human interaction, which is subject to error and are generally not recommended for high volume tax filing transmissions.

- The manual process of filing tax reports doesn’t end with the completion of uploading files to the website. PSPs must also monitor acknowledgement response files from the agency, to confirm

receipt of the file and a confirmation number, and to also record error messages from the initial file. The PSP must then work with their internal teams and or clients in order to make corrections, resubmit rejected files, confirm receipt, and record any subsequent error messages.

- Browser-based file uploads rely on human interaction with the agency's website. To accommodate mandated use of browser-based systems, complicated scripts must be developed by the PSP to automate this interaction. Sometimes automation is prohibited and blocked by the taxing authority's security protocols, such as CAPTCHA. When the automation is blocked, PSPs must rely on human intervention for these high-volume, frequent and high-risk transactions which increases the opportunity for error with bulk filings. A single error could impact hundreds or thousands of employers since PSPs are mostly transmitting batch files.
- Browser-based systems are difficult to maintain because of the need to communicate and coordinate routine website changes (e.g., screen layouts). Any time changes are made to the agency's website, even minor changes, the scripting programs must be modified to simulate human interaction to incorporate the new web page functionality, and reprogram the script for the additional steps necessary to capture data returned by the tax authority, such as acknowledgements and error messages.
- When using security measures to detect and prevent access by bots from unknown parties, the state may unintentionally implement security features that restrict known and trusted PSPs from accessing the state website using high-speed automation that's necessary to support their clients. CAPTCHA* is an example of a security feature that may help deter unknown parties from accessing state websites, but also blocks automation from trusted parties. Acceptable security options include:
    - IP address accept listing or allow listing in order to bypass security measures intended for individuals (i.e. CAPTCHA*).
    - Coordinating an exchange of secure keys with trusted partners.
    - Browser security certificates, such as Identrust that is used by the IRS, might be worth considering. Some vendors maintain them for up to 3 years before expiring.

Web Browser Technical Specifications

- 1) Point-to-Point transmission over HTTP with SSL
    - HTTP over SSL through basic authentication and basic form upload/download of compressed/encrypted payloads: The normal protocol for secure web pages exchange; it can be used to send/receive compressed/encrypted electronic filing submissions.
        - The tax agency needs to publish the specifications of the compression/encryption methods (e.g. PKZIP/WINZIP or PGP).
        - Exchanged compressed/encrypted files should not exceed 4MB (practical limitation in order to minimize transmission times and reduce likelihood of transmission interruptions).
- 2) Interactive Electronic Filing over HTTP with SSL
    - Unattached transmission and processing is much preferred by bulk processors (which includes both the P2P and A2A options described above) over the web browser file upload option.

- This alternative is not appropriate for high volume filers since file sizes (even compressed files) larger than four megabytes (for Unix-based servers) or two to three megabytes (for Windows-based servers) are not recommended.
- Given the volume of employers that service providers represent, it could take several days or weeks to upload many small files using a web browser upload transmission process.
- The integrity of the electronic filing is questionable when there is an interruption in connectivity. Both the bulk provider and the agency have to go through extensive manual processes to determine which employers were successfully reported, and which employers still need to be transmitted.

Other Web Browser Considerations

- **Password Resets:** Some websites when they are locked out require that an administrator of the PSP call to reset passwords. For large PSPs, it would be helpful to allow multiple administrators so multiple team members can call to reset the password.
- **Administrator Changes:** Allow for the ability to change administrators when there are role changes at the payroll firm without needing to reauthorize all employer-clients under the new administrator. Some state websites don't allow the administrator to be updated, and all employer clients must be reauthorized under the new administrator, even though the clients are still clients of the same PSPs.
- **System Performance for PSPs:** If PSPs are able to gain access to view their client-employer accounts online, consider the system performance of the web pages that display multiple employers. PSPs experience extreme slowdown once they've added several hundred or thousands of clients to their profile, and at times, the slowdown renders the websites to be useless for the PSPs resulting in more phone calls and emails to the state agency.
    - **Recommendation:** Monitor page load responsiveness and make routine enhancements to ensure the website is performing as expected.
- **Authorization of PSP:** Third-party authorization should not be required in order to file and pay on behalf of an employer since the third-party is only pushing information to the tax administrator. If third-party access is required for other actions beyond filing, then the tax authority should notify the employer when a third party has requested access to the employer's online account, but not require that the employer approve or deny the request. After sufficient time has passed (i.e. 10 business days), if access hasn't been denied by the employer, then basic view and file/payment access should be granted to the PSP in order to optimize usage of the online features that have been created. The website should also allow the employer to see who has been granted access to view their account so that they can manage active third-party and internal users. The employer should be able to grant additional permissions (administrator roles, etc.).
    - **Example agency with this functionality:** Michigan Unemployment Insurance Agency.
- **Two-factor authentication (TFA):** NPRC members prefer that the state offer an option to send a TFA code to an email address. A current trend is to only allow codes to be sent to mobile phone numbers via text messages or via mobile authentication applications. Many PSP's security teams restrict users from using their personal mobile phones for conducting business. Allowing a code to be sent via email allows for the PSP representatives to retrieve the code using company issued and approved computers.

**CAPTCHA as a Security Tool*

- CAPTCHA is a tool that is added to a web page to determine whether a user is a bot or a human. It invokes a confirmation measure known as challenge-response authentication, by asking the user to complete a simple test that proves you are a human. Typically, these come in the form of a distorted series of letters and or numbers or images to be selected based on a prompt.
- However, all CAPTCHA can confirm is that the person accessing the CAPTCHA sequence is a person and not a bot. It can't validate that the person is who they say they are and is therefore not really a security measure as it doesn't provide an answer to a significant security question: "is this a trusted person for this site."

Contacting NPRC

NPRC members are very interested in working with all state tax authorities to develop secure and efficient next generation systems for wage and tax reporting. Please let us know how we might assist in addressing these issues. If there are additional questions about secure electronic processes, please contact NPRC at nprc@nprcinc.org.

References

Rutter, T (2005) CAPTCHA are not a security measure

Pankov, N (2021) RIP CAPTCHA

Young, L (2021) Building a WebAuthn Click Farm - Are CAPTCHAs obsolete?