REQUEST FOR INFORMATION

COMMON TRANSMISSION SYSTEM

THE DEADLINE FOR THE RECEIPT OF RESPONSES IS: 27 MARCH 2023 – 6.00 PM PARIS TIME

Contact email: cts-consultations@oecd.org

URL: https://www.oecd.org/callsfortenders/listofallcallsfortenders.htm

Preamble

The OECD brings together the governments of countries committed to democracy and the market economy from around the world to:

- Support sustainable economic growth
- Boost employment
- Raise living standards
- Maintain financial stability
- Assist other countries' economic development
- Contribute to growth in world trade

The OECD also shares expertise and exchanges views with more than **100 other countries and economies**, from Brazil, China, and India to the least developed countries in Africa.

Fast facts

Established: 1961
Location: Paris, France
Membership: 38
Budget: EUR 421 million (2020)
Secretariat staff: 3300

Secretary-General: Mathias Cormann
Publications: 250 new titles/year
Official languages: English/French

Monitoring, Analysing and Forecasting

For over 60 years, the Organisation for Economic Co-operation and Development (OECD, hereinafter referred to as "OECD" or "Organisation") has provided statistical, economic and social data comparable with the most important and most reliable in the world. In addition to its collection of data, the OECD monitors trends, analysis, and forecasts economic developments. The Organisation studies changes and developments in trade, environment, agriculture, technology, taxation and more.

The Organisation provides a setting where governments can compare their experiences in developing public policies, seek answers to common problems, identify good practices and coordinate both domestic and international policies.

Enlargement and Key Partners

The Organisation has open accession discussions with Brazil, Bulgaria, Croatia, Peru and Romania, and is also reinforcing its engagement with its Key Partners – China, India, Indonesia and South Africa.

Publishing

The OECD is one of the world's largest publishers in the fields of economics and public policy. OECD publications are a prime vehicle for disseminating the Organisation's intellectual output, both on paper and online.

Publications are available through the OECD Network Environment (**O.N.E**) for government officials, through OECD iLibrary for researchers and students in institutions, corporate, subscribed to our online library for individuals who wish to browse titles free-of-charge and also to purchase publications.

1 Introduction and Objectives of this Request for Information

Introduction

1. In 2015, the OECD's Forum on Tax Administration (FTA) which brings together more than 50 of the most advanced tax administrations from around the world, asked the OECD to develop a transmission system that would allow tax administrations to securely exchange tax information with each other. On that basis, the OECD launched a call for tenders and selected an industry supplier to build the OECD Common Transmission System (CTS).

2. The CTS was developed in 2016 and the first half of 2017 and went live in September 2017. Initially, the scope of use of the CTS was limited to the automatic exchange of offshore financial account information pursuant to the OECD's Standard for Automatic Exchange of Financial Account Information in Tax Matters (often referred to as the Common Reporting Standard), as well as the exchange of information on corporate tax transparency matters under the OECD project on Base Erosion and Profit Shifting (BEPS).

3. At present, 110 tax administrations are using the CTS for transmissions of the above information types. Furthermore, the current version of the CTS "2.0", activated in February 2021, allows for the exchange of 25 types of tax information in total.

4. The contract with the current supplier will terminate no later than the end of November 2026.

5. The OECD is planning to issue a comprehensive Call for Tenders (CfT) in early 2023 to deliver the new version of the CTS "3.0", well in advance of the end of the existing contract, in order to allow for an orderly handover including with respect to all of the CTS users.

6. In advance of the CfT, using a Request for Information (RFI), the OECD wishes to identify the market's interest in participating in the CfT, as well as to obtain the market's view on potential evolutions that are being discussed for the CTS. This RFI is entirely non-binding for the OECD and does not represent a commitment of any kind towards interested companies.

Objectives of the Request for Information

7. The core functionality of the CTS, to enable the secure transmission of tax information between tax authorities, will need to be maintained. Furthermore, since the development of the original version of the CTS in 2016 there have been major developments in the IT environment: massive adoption of webconference systems, development of blockchain technologies, post-quantum cryptography advances, etc.

8. The OECD needs to ensure that the CTS architecture is optimal from a functional and security perspective. The OECD considers that some of the IT developments cited above, might be beneficial for the jurisdictions using the CTS and therefore, it is requesting industry's feedback regarding more efficient, secure, and functional technical developments that can support the development of the new release of the CTS.

9. The objectives of this Request for Information (RFI) are:

1. To determine the industry capacities and capabilities that can be leveraged to deliver the CTS core functionality more efficiently and securely (**Core functionality**)
2. To assess the readiness and capacity of industry to implement a practical solution that includes secure communications using post-quantum transmission cryptographic algorithms (**Quantum functionality**), including support for jurisdictions to adopt quantum-safe cryptography (change management, software development and preparation of business cases)
3. To evaluate the capability of the industry to provide secure and compatible systems for real-time videoconferencing and data sharing between tax administrations in a multilateral environment (**Real-time functionality**) handling confidential information.

10. **Respondents may respond in relation to all or some of the objectives highlighted above.**

11. Please submit your responses by filling in the attached document "RFI – Annex A – Answering.docx" and sending it to cts-consultations@oecd.org

Additional information can be found in https://www.oecd.org/callsfortenders/listofallcallsfortenders.htm

2 Nature of the RFI

12. This RFI is neither a CfT nor a Request for Proposal (RFP). No agreement or contract will be entered into based on this RFI. The issuance of this RFI is not to be considered in any way a commitment by the OECD, nor as authority to potential respondents to undertake any work that could be charged to the OECD. This RFI is not to be considered as a commitment to issue a subsequent solicitation or award contract(s) for the work described herein.

13. Participation in this RFI is encouraged but is not mandatory. There will be no short-listing of potential suppliers for the purposes of undertaking any future work because of this RFI. Similarly, participation in this RFI is not a condition or prerequisite for the participation in any potential subsequent solicitation.

1. Use of Responses: although the information collected may be provided as commercial-in confidence (and, if identified as such, will be treated accordingly by the OECD), the OECD may use the information to assist in drafting performance specifications (which are subject to change) and for budgetary purposes.
2. Confidentiality: The RFI and any further information communicated to the respondent or to the OECD, or which come to their knowledge in the course of RFI are confidential and are strictly dedicated to the purpose of the RFI. The OECD or the respondent reserves the right to request to have all documents and information and copies, regardless of the format, to be returned at the end of the RFI process or to receive a written attestation that they have been destroyed.
3. Cost: RFI are not paid. No reimbursement of expenses related to the preparation of any response to this RFI will be made by the OECD.
4. Deadline: The RFI closing date published herein is not the deadline for comments or input. Comments and input will be accepted any time up to the time when/if a follow-on solicitation is published.

3 Core functionality

Current Solution Description

Background

14. The OECD has developed a number of international policies for the exchange of tax information between tax authorities, including the Common Reporting Standard (CRS), Country-by-Country Reporting (CbCR), Exchanges on Tax Rulings (ETR), exchanges of Digital Platform Information (DPI), Exchanges of Information on Request (EOIR), the Crypto-Assets Reporting Framework (CARF), etc. (the Policies[1])

15. The Policies require the collection by tax authorities of diverse types of tax information in relation to taxpayer activity, which is then subsequently exchanged via the CTS on a periodic basis with other relevant tax authorities internationally. Pre-determined XML formats and file preparation requirements have been developed for jurisdictions to prepare the information and ensure that the data is kept confidential and encrypted during transmission.

16. The CTS is a production system used daily by 110 jurisdictions. Although exchanges of tax information happen during the whole year, the number of exchanges changes from one month to another and there are peak periods in the year when significantly more files are exchanged.

17. The CTS enables the exchange of tax information by providing a means for tax authorities to transmit files. It is only a system used for transmitting files and **does not store or backup information beyond the time is required for one jurisdiction to retrieve the information sent or uploaded by another jurisdiction.**

Current Implementation

18. For information purposes, this section describes the current CTS implementation.

19. The CTS consists of two identical environments: Conformance, used by tax authorities for testing and validation, and Production used by tax authorities for the actual exchange of information. A third development environment, not available for users, is used by the current supplier to develop new features.

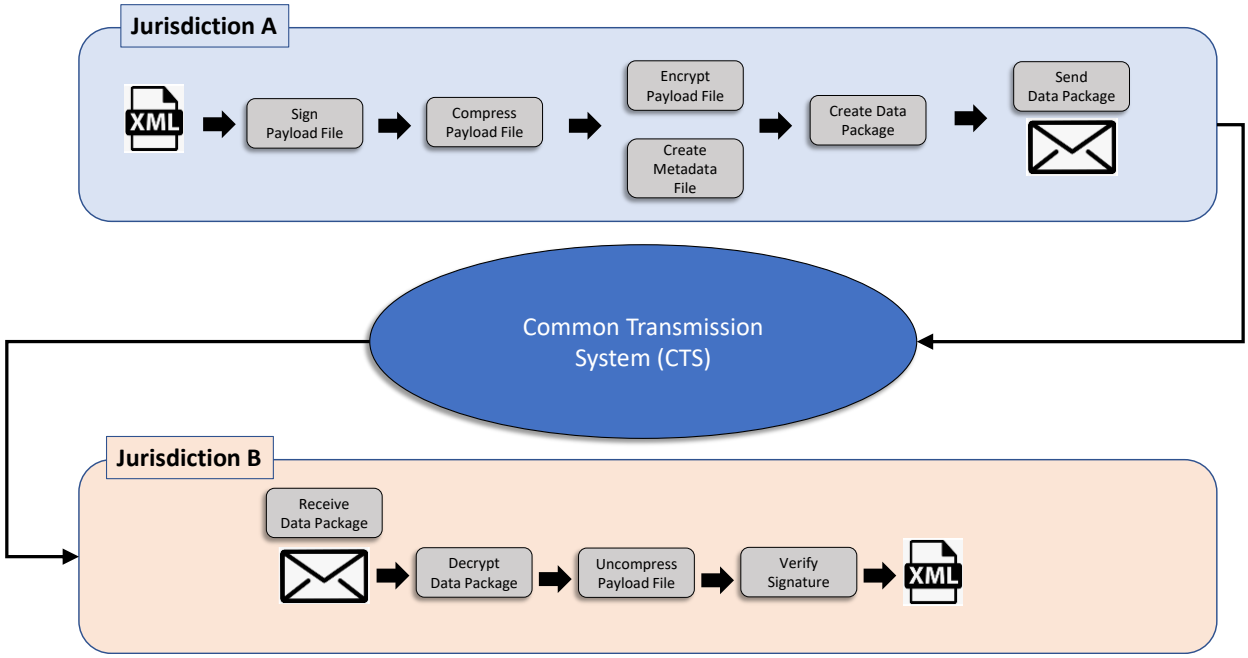
20. Jurisdictions package the tax information at source. The information is encrypted specifically for each of the receiving jurisdictions, leveraging symmetric and asymmetric cryptography. Only the metadata, used to correctly route the data between the jurisdictions, is visible to the CTS system.

[1] Exchange of information - OECD

21. Information sent through the CTS is always encrypted by the users prior to it being sent. The data security of the CTS is based on a hybrid encryption[2] scheme that uses both asymmetric and symmetric encryption mechanisms. Jurisdictions connect to the CTS and upload their encrypted information using HTTPS or SFTP protocols.

22. The following diagram describes the main steps in data preparation and processing:

Figure 3.1. Common Transmission System. File Preparation and Processing.



23. The element of the process that is the subject of the RFI is the actual transmission of the information between tax administrations (the "pipe" or CTS). This therefore does not include data storage or file preparation prior to the sending of the information or any processes following the receipt of the data (e.g., relating to encryption, compression, storage etc.), which is provided for information.

24. The building blocks of the current CTS implementation are:

Users' interface

Users interact with the CTS through several sub-interfaces

1. Transmission interfaces

   The transmission interfaces are used to send and receive information through the CTS. The protocols that can be used are:

   a. HTTPS for manual upload/download of information
   b. SFTP (push and pull), for automated upload/download of information
   c. REST API: used exclusively to download public certificates of partner jurisdictions. It is not possible to upload or download data packages via the REST API.

2. Information gathering interface

   The information gathering interface is a Rest API providing:

[2] Hybrid cryptosystem - Wikipedia

a. information to a sending jurisdiction regarding the transit status of a data package as well as the CTS Transmission ID of any of its sent transmissions, based on its file name and file ID.
b. a list of files available for downloading for the user
c. information on the status of an Authorized Transmission [3]

3. Reporting interface

   Extensive reporting is provided as part of the solution. It concerns the type of information sent/received, based on the meta-data, the number of files, etc.

4. Administration interface

   The administration of the users in the jurisdictions who can access the Solution and their roles is performed via a web interface

5. Alerting interface

   The solution sends email alerts corresponding to different events to inform of different events (file available, file downloaded, file about to expire, etc.)

   Users can subscribe to different types of alerts based on their profile and preferences.

Encryption, signature, identify, and data retention

Data encryption is the ultimate layer of security in the CTS. Encryption is handled at jurisdiction level and the CTS has no visibility whatsoever of the encrypted data.

Packages addressed to a specific jurisdiction are signed using the private key of the sending jurisdiction and encrypted using the public key of the destination jurisdiction.

The jurisdictions' identities are ensured via public Extended Validation SSL (EVSSL) certificates, which are purchased by the jurisdictions through a list of pre-validated Certification Authorities.

Tax data is held encrypted on the CTS for the minimal amount of time required to download the information or to push it to the receiving jurisdiction.

Security

The data transmitted through the CTS consists of encrypted confidential taxpayer information. Security is therefore of critical importance to the CTS. For confidentiality reasons, it is not possible to provide a full description of all the IT security mechanisms, but they include all of the layers that can be expected to be found in a critical application: Firewalls, Intrusion Prevention/Detection Systems (IPS/IDS), Web Application Firewalls (WAFs), IP filtering, Multifactor Authentication, etc.

Likewise, security is integrated at business level. Jurisdictions can limit the time interval and the type of data (e.g., CRS, CbCR, etc.) that their users are authorized to send or receive from each of the partner jurisdictions via a mechanism called Authorized Transmissions.

Suppliers are certificated to manage highly confidential information and possess recognized certification in the field of IT security.

Finally, there are governance frameworks in place in respect of the operation of the CTS and the relations with the jurisdictions, in order to maximise the security.

Add-on services

[3] An authorized transmission is a security mechanism at business level. It prevents a jurisdiction from sending or receiving a type of tax information to or from a jurisdiction with which there is no agreement to exchange information.

The current implementation includes several services aimed to ensure the correct functioning and security of the system, notably a 24x7 helpdesk and security monitoring of the platform. Escalation and governance mechanisms are also in place.

25. The system supports both high-frequency-low-volume exchange (the exchange of information on request) and low-frequency-high-volume exchanges.

26. There are 110 jurisdictions using the system, which all have the capability to be senders and receivers of information.

27. The volume of transactions is around 150 000 per year with a perspective of increasing the number in the coming years with the adoption of the new Policies for the exchange of information. The maximum estimated number of yearly transactions for the project is under 1 000 000 per year.

28. The size of the files to transmit is up to 250 MB, but most jurisdictions have set a lower limit (100 MB).

29. Core Business Rules

The CTS has been developed to satisfy the following main Core Rules, which are still of mandatory compliance and will be required for any new implementation of the CTS (the System):

1. The System will need to be up-scalable to accommodate further jurisdictions joining the exchange of information under the Policies. It must also allow for the exchange of information between tax administrations in relation to other Policies that might be developed.
2. There shall be a policy for ensuring the legal protection of the data transmitted and subject matter access, including the definition of the moment in time at which the transmission of ownership occurs.
3. There shall be a commonly agreed policy towards the minimum standards for warranting confidentiality, encryption, integrity, and non-repudiation of data transmissions through the CTS.
4. The files to be sent through the CTS shall be subject to minimum common file format and preparation rules.
5. There must be controls over identity and user access to the System, with only authorised users being permitted to use it.
6. The System must be available internationally and 24 hours a day / 7 days a week.
7. The System shall only transmit the data, not store the data, except for pre-defined minimal file retention periods required to complete the transmission.
8. The System will be supported, supervised, and managed by the supplier.
9. Users will have the possibility to parameter certain components of the System (e.g.: creating users, defining Authorized Transmissions)
10. There will be an alerting and reporting system to inform of new and historical transmissions.

30. The CfT will provide a detailed list of features of the current CTS implementation to scope accurately the proposed solution.

Core Functionality Evolution

31. The areas identified in the current system that could be addressed differently and that the OECD is interested in exploring are:

1. Reliance on external Certification Authorities to validate the identity of the jurisdictions. Jurisdictions must liaise with external third-party companies and request certificates with specific security features. The OECD validates the certificate before allowing jurisdictions to use them in the system.

   Certificates have increasingly short validity periods and increasingly longer size keys are required to ensure the security of the system.

   Reliance on external Certification Authorities externalises the management of part of the CTS security and trust to a third-party and introduces complexity to the onboarding and administration of the system
2. Enhancements to the administrators' logging system, such as immutable audit logs.

32. Lastly, the current system is designed on a peer-to-peer configuration. The OECD would be interesting to explore the possibility to exchange using a peer-to-multi peer approach.

Expected Outcome for the Core Functionality of CTS 3.0

33. The OECD is looking for **high-level information** on the capacity of potential suppliers to either develop a system that would meet the functional description detailed under Current Solution Description or to instead adapt an existing system accordingly. Likewise, the OECD is also interested in potential solutions that can expand the Core Functionality and integrate the functionalities detailed under Core Functionality Evolution.

34. **The OECD is not prescribing any solution or technology to be used to deliver the Core Functionality**, it will be up to the supplier to select the most adequate technical solution, but in order assess the feasibility of this project is very important that the focus is put on two elements:

1. How the proposed system will maintain the current level of functionality (Core Business Rules) and the existing user interfaces (especially the transmission, information gathering and alerting interfaces),
2. describing the technical features of the new system, estimating the time it would take to develop such a system and associated costs. While precision is preferable, estimates could also be presented in ranges or as high-level qualitative descriptions.

35. Jurisdictions have invested heavily in the development of their internal systems**. A basic constraint of any proposal is that some parts of the user interface, notably those that have been heavily automated (transmission, information gathering and alerting), must be preserved.**

During the procurement process that will follow this RFI, the OECD will be able to provide the existing technical specifications for those interfaces.

4 Quantum functionality

36. In addition to obtaining information from potential suppliers in relation to the future delivery of the Core Functionalities, the OECD wants to explore possible solutions to address future security threats to the CTS. Jurisdictions use the CTS to exchange information for tax purposes. Due to its sensitive nature, the information needs to be kept confidential. Encryption acts as the ultimate layer of security and ensures that only the intended partner jurisdictions will have access to the confidential information in the file.

37. The cryptographic algorithms used to encrypt and sign the information transmitted via the CTS were defined in 2016 by the OECD jointly with the jurisdictions and are based on asymmetric (RSA-4096) and symmetric cryptography (AES-256).

38. A potential future threat that has been identified to the cryptography used in the CTS (or to any other IT system using RSA or elliptic-curve cryptography (ECC), such as online banking) comes from Quantum Computers, which are computers that function using the principles of quantum mechanics.

Quantum computers, armed with a quantum algorithm known as Shor's algorithm, could quickly solve the factoring problem and the discrete logarithm problem which underlie the security of most of the public-key cryptography used today, including the CTS' cryptography.

39. Although there is no immediate threat, as we have still several years before a working quantum computer becomes available, the CTS might become vulnerable to a family of attacks known as "store now, decrypt later", where a hacker intercepts the information now and waits until there is a quantum computer available to decrypt it[4].

40. The OECD wishes to anticipate any potential threat coming from Quantum Computers by making sure that the CTS 3.0 is "quantum-ready". Four strategies have been identified to tackle this future threat:

1. Use quantum-resistant asymmetric algorithms[5]. Either by directly replacing existing algorithms or using a hybrid approach combining both Post-Quantum Cryptography and established classical schemas (as recommended by agencies such as BSI or ANSSI).
2. Implement crypto-agility, which will allow for the change to the existing cryptographic algorithms without requiring a major overhaul of the CTS or of the jurisdictions' infrastructure.
3. Use a system based only on symmetric algorithms, which are supposed to be resistant to any quantum attack, provided the key is long enough.
4. Migrate the entire transmission stack to a quantum-native solution (e.g., QKD[6]), although it is a technology under development and at the moment there is no general consensus that it is or can be a valid and secure solution.

[4] https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/
BSI - Quantum Technologies and Quantum-Safe Cryptography (bund.de)
Preparing for Quantum-Safe Cryptography - NCSC.GOV.UK
Post-Quantum Cybersecurity Resources (nsa.gov)

[5] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

[6] QKD: Quantum Key Distribution

Expected Outcome for the Quantum Functionality

41. The OECD is looking for suppliers with the following capabilities:

1. Expertise to analyse the existing implementation of the CTS 2.0 and define the technical requirements and the implementation roadmap to ensure that the CTS is safe against quantum computing attacks.
2. Expertise to propose a path for the implementation of "crypto-agility" to evolve rapidly the cryptographic algorithms
3. Expertise to design and evaluate alternative architectures to the current design, which will natively ensure the resistance against quantum-attacks.

42. As a first step, the OECD is looking for high-level information on the capacity of potential suppliers to analyse the risks and help with implementing Post-Quantum Cryptography in the existing CTS 2.0.

43. Potential suppliers will have significant expertise with cryptographic implementation projects. This will allow them to either help jurisdictions with implementing the new algorithms in their systems directly, or with introducing an intermediate layer in different phases that would add the required quantum security as proposed in the diagrams below.

Figure 4.1. Example of intermediate layer to enhance resistance against quantum algorithms within the CTS

Phase 1: the intermediate layer is implemented at the CTS system avoiding changes in all jurisdictions

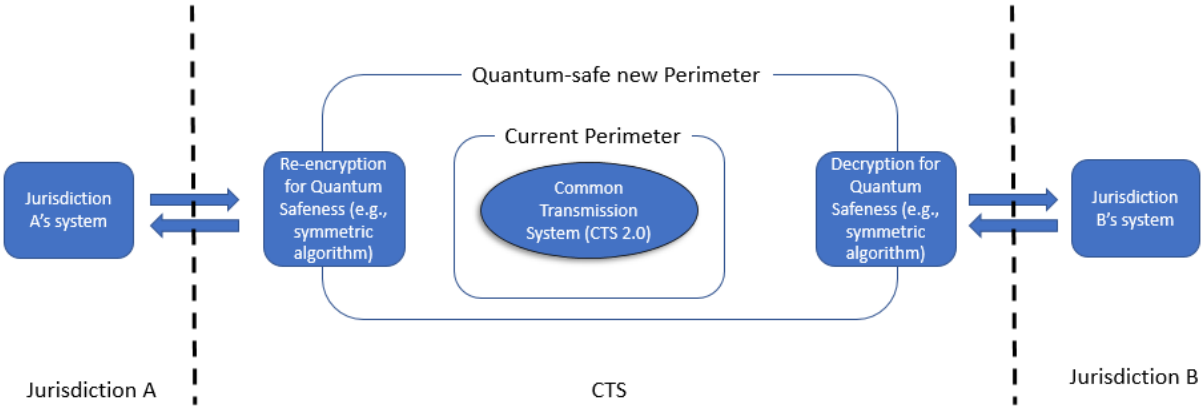
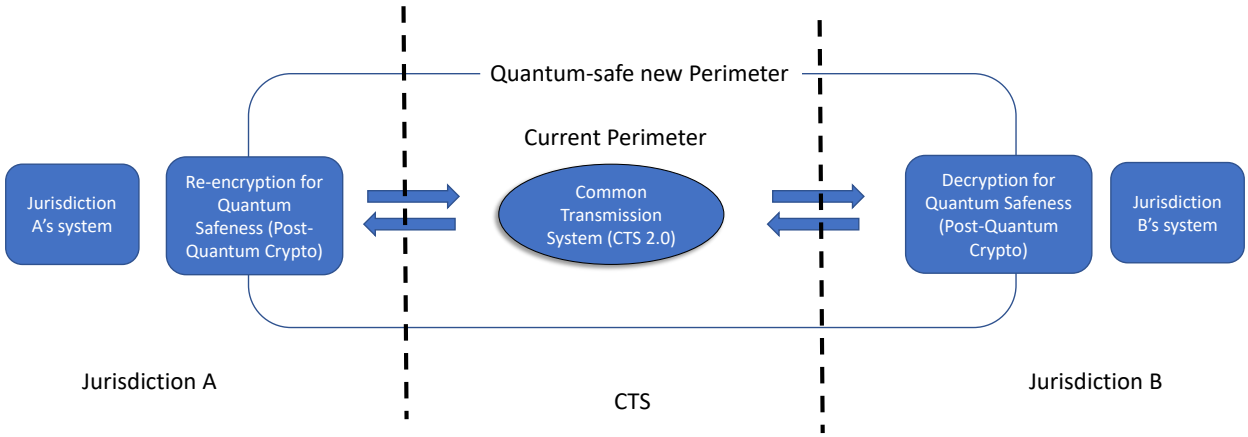


Figure 4.2. Example of intermediate layer to enhance resistance against quantum algorithms at jurisdiction level using Post Quantum Cryptography

Phase 2: the intermediate layer is implemented at the jurisdiction boundary, protecting the system from store-and-decrypt attacks by the CTS supplier (zero-trust approach).



44. It is expected that the suppliers have experience in explaining complex technical issues to different non-technical stakeholders, such as the risks stemming from quantum computers and can help jurisdictions build business cases as required.

45. In a second phase, the OECD wishes to develop the current model towards "crypto-agility". "Crypto-agility" will allow jurisdictions to develop more easily their cipher suites currently used in their systems with minimal impact to their business operations. The expectation is to be able to adopt crypto-agility as part of CTS 2.0.

46. Finally, the OECD is looking for input in possible radically different designs that could be adopted as part of tackling the future quantum threat to the CTS 3.0, notably:

- Possible implementation plans using only symmetric algorithms.
- Design requirements to consider using quantum transmission technologies.
- Risk-benefit analysis of the different designs (Post-Quantum Cryptography, only symmetric algorithms, quantum transmission or a mix).

5 Real-time functionality

Background

47. Over the last years, tax administrations around the world have invested significant amounts to digitalise their processes. Important dimensions of this work are making the interactions between tax administrations and taxpayers more efficient and interactive and enhancing the tax audit and compliance verification activities of tax administrations.

48. In the international context, this includes the digital sending of files containing tax information through the CTS, but digital communication is also increasingly relied upon to permit videoconferences between tax administrations and to allow tax compliance activities to be carried out collaboratively between two or more tax administrations (and affected taxpayers) with the support of a virtual data room.

49. At the same time, experience in recent years has shown that there is currently no single videoconferencing platform, or virtual data room, which can be used by all tax administrations. The reasons are multiple and range from IT security and compliance to licensing cost or other internal operational or technical factors.

50. Whether as part of the Common Transmission System or as a standalone functionality, the OECD would like to identify potential solutions that would allow tax administrations to hold secure and confidential discussions through a common videoconferencing platform.

51. In addition, the OECD would like to explore options for the collaborative sharing of, and working on, taxpayer-specific, confidential documents between tax administrations in a real-time manner, and a secure encrypted end to end user email. This is particularly important for ensuring the efficient administration of complex tax compliance processes, such as in the framework of advance tax certainty programs for large multinational corporate taxpayers.

52. **Suppliers are free to suggest solutions to some or all of the following aspects: videoconferencing, the virtual data room and secure email.**

Main challenges

53. The main challenges for any type of real-time communication that have been identified are:

1. Data sovereignty, i.e., the requirement that data is always treated in compliance with the laws of the jurisdiction that has collected the data.
2. Operational sovereignty, i.e., the requirement that an external supplier cannot compromise the jurisdiction's data. In other words, the jurisdiction owning the data keeps full visibility and control over the supplier's operations related to its data.

Solution Requirements

54. At this moment, there are no specific requirements beyond addressing the main challenges described above. Technical and security requirements, such as type of encryption or proxy compatibility, can be analysed in a second phase once the technical specifications of a possible solution are known.

55. This means that, as long as the main challenges are addressed, at this stage all options can be proposed and will be considered, including:

- Use of public/private webconference solutions;
- installation of dedicated equipment in tax administrations;
- implementation of ad-hoc procedural mechanisms to ensure operational sovereignty.

Volume estimations

56. The maximum number of participants in secure videoconferences is estimated at 100 simultaneous participants.

57. The adoption of secure videoconference and virtual data room solutions is expected to increase gradually as tax administrations adapt their IT systems to connect to the new infrastructure. It is expected that this project will ultimately lead to wide-spread usage by the tax administrations, but at this stage is difficult to anticipate the number of videoconferences or a volume of data uploaded to a virtual data room.

58. Suppliers should provide price indications based on an estimated number of videoconferences and volume of data uploaded to a virtual data room.

Expected Outcome for the Real-Time Functionality

59. The OECD is looking for high-level information on the capacity of potential suppliers to develop a new system, or to adapt an existing system, to provide a secure videoconference solution and/or virtual data room for use by tax administrations and/or secure encrypted end-to-end email.

60. The OECD is especially interested in business cases that have been implemented and proof-tested to address the same requirements in other environments facing similar confidentiality and cross-border collaboration issues, such as in the military, law enforcement or healthcare domains.

61. Ideally, the OECD would like to have also financial estimates and real-life references of implementations to better frame the upcoming Call for Tenders.

6 Timeframe and Business model

Timeframe

62. Responses to this request for information are required by 27 March 2023. These responses will inform a Call for Tenders with expected publication date by 30 June 2023.

63. The timeframe to deliver the required functionalities in this document are:

1. Core Functionality:

   The new version of the CTS would need to be fully developed by the end of February 2026, to allow for user access and testing and in good time before the first transmissions with the new system in September 2026.

2. Quantum Functionality

   Cryptographic agility and/or quantum-resistant algorithms are expected to be developed in the next few years. It is expected that new systems to deliver the Core Functionality are designed with the Quantum requirements in mind, so the Solution can be evolved toward a quantum-attack resistant solutions (support for post-quantum cryptography implemented at jurisdiction level, quantum-native technology or symmetric-only encryption) by design.

3. Real-time Functionality

   Real-time functionality requires a completely different set of IT tools and infrastructure and is considered a different workstream.

   It is expected that the functionality could be needed as early as in 2024.