TECHNICAL ASSISTANCE REPORT

LIBYA

Workshop on Tax Administration Digitalization in Fragile and Conflict-Affected States

JANUARY 2025

PREPARED BY

Fadia Sakr, Sabine Corm, Joshua Aslett, Paulo Paz, Gustavo Figueiredo and Rivelino Patrício

MEMBERS

Afghanistan, Algeria, Djibouti, Egypt, Iraq, Jordan, Lebanon, Libya, Morocco, Sudan, Syria, Tunisia, West Bank and Gaza, Yemen

DEVELOPMENT PARTNERS

European Union, France, Germany, Netherlands, Saudi Arabia, Switzerland

The contents of this document constitute technical advice provided by the staff of the International Monetary Fund to the authorities of Libya (the "CD recipient") in response to their request for technical assistance. Unless the CD recipient specifically objects to such disclosure, this document (in whole or in part) or summaries thereof may be disclosed by the IMF to the IMF Executive Director for Libya, to other IMF Executive Directors and members of their staff, as well as to other agencies or instrumentalities of the CD recipient, and upon their request, to World Bank staff, and other technical assistance providers and donors with legitimate interest members of the Steering Committee of METAC (see Staff Operational Guidance on the Dissemination of Capacity Development Information). Publication or Disclosure of this report (in whole or in part) to parties outside the IMF other than agencies or instrumentalities of the CD recipient, World Bank staff, other technical assistance providers and donors with legitimate interest members of the Steering Committee of METAC shall require the explicit consent of the CD recipient and the IMF's Fiscal Affairs department.

International Monetary Fund, IMF Publications
P.O. Box 92780, Washington, DC 20090, U.S.A.
T. +(1) 202.623.7430 • F. +(1) 202.623.7201
publications@IMF.org
IMF.org/pubs

MEMBERS


Afghanistan


Algeria


Djibouti


Egypt


Iraq


Jordan


Lebanon


Libya


Morocco


Sudan


Syria


Tunisia


West Bank and Gaza


Yemen

DEVELOPMENT PARTNERS


European Union


France

Germany


The Netherlands


Saudi Arabia


Switzerland

Contents

I. Summary of Workshop Activities

1. The International Monetary Fund (IMF) held a workshop to explore tax administration digitalization in fragile and conflict-affected states (FCS). Delivered jointly by the IMF Fiscal Affairs Department (FAD) and the Middle East Technical Assistance Center (METAC), the workshop centered around sharing country experiences, discussing the fundamentals of tax administration, and exploring an innovative option for digitalization. Held at the Cairo Marriott Hotel & Omar Khayyam Casino in Cairo, Egypt, from November 30 to December 3, the event was facilitated by IMF staff Ms. Fadia Sakr, Ms. Sabine Corm, Mr. Joshua Aslett, and Mr. Paulo Paz, and short-term IMF experts Gustavo Figueiredo and Rivelino Patrício, with participants from Iraq, Libya, and Yemen (Annex I).

2. The workshop follows from a webinar on digitalization held by METAC in April 2024. The webinar was divided into four sessions that provided (a) regional insights into digital tax administration; (b) essential capabilities of a modern integrated tax administration system (ITAS); (c) key reforms required to support digitalization; and (d) an overview of the "Kontaktu" platform, an innovation from the IMF in the form of an IT platform approved for use in FCS states. The concluding Q&A session proved highly interactive, with many questions raised that focused on Kontaktu's specific technology, functions, and implementation processes. Subsequently, METAC received and followed up on detailed questions received from participants regarding the platform's technical aspects.

3. The workshop sought to explore the suitability of the Kontaktu IT platform for the digitalization of participant countries' tax administrations. Accordingly, at the workshop's outset participants were encouraged to maintain objectivity throughout the event with full consideration for typical models of tax administration digitalization (acquisition of a commercial ITAS or in-house, custom IT development; and the different models for financing and support). The goal of the workshop was to help support a decision as to whether the Kontaktu option may or may not be productive in each country's unique circumstances. To that end, representatives of the three countries presented their tax systems, main taxes, and current stage of digitalization. The IMF team in turn provided details on the Kontaktu platform, led discussions related to taxpayer obligations (registration, filing, and payment), and explored Kontaktu's capabilities in data gathering, analysis, and dashboard construction.

4. The IMF will support member countries' digitalization efforts independently of their choice of specific IT platform. For those countries that express further interest in Kontaktu, follow-on support from the IMF to help scope implementation projects can be provided. These projects might involve elements of self-financing from participant countries and could also make use of support from development partners. The IMF in turn can support customization, deployment, knowledge transfer, and handover of the platform. For the countries wishing to explore this option further, a formal request will be required to initiate the process. If Kontaktu is determined not to be suitable, the IMF will remain available regardless to continue to provide support on digitalization.

II. Digitalization as an Imperative for Efficient Revenue Mobilization

5. Digitalization has become essential for domestic revenue mobilization and efficient tax administration. To manage complex tax operations, tax administrations are adopting compliance risk management (CRM) strategies to utilize limited resources most efficiently. CRM relies on comprehensive data sets to identify, rank, and prioritize key tax compliance risks, and modern IT systems are crucial for gathering and matching these data sets. Equally important, modern technology can offer broad access to simpler services for taxpayers to fulfill their basic tax obligations around registration, filing, payment, and accurate reporting. Digitalization also plays a vital role in enhancing transparency and reducing corruption within tax administrations. While the benefits of digitalization are clear, the process of digitalizing can be very challenging. Today, there are two established paths.

A. Established Paths to Support Digitalization of Tax Administrations[1]

6. Acquisition of a commercial-off-the-shelf Integrated Tax Administration System (ITAS) is one option. These products generally cover comprehensive work streams and provide electronic services to taxpayers along with internal modules that support core business functions within administrations. However, they can be expensive, may require a complex procurement process, and entail medium to long-term commitments. Typically, these off-the-shelf IT systems have limited flexibility (or are expensive to customize) and are designed primarily for stable tax environments. Because of the rigidity and expense of these products, it is not unusual for jurisdictions to adapt their tax systems to fit the IT solutions. Despite the challenges, quality ITAS options exist that are mature and well-tested in actual operations.

7. A second option is to develop in-house IT systems. This approach can allow for the design of IT systems tailored specific country needs and enable progressive implementations with a greater degree of flexibility. The disadvantage is that it can take more time to develop and deploy a high-quality system, requiring solid and stable sponsorship. The associated risk of lack of experience can be mitigated with technical assistance in designing the project and IT system, benefiting from international good practices.

8. Both options can be challenging for FCSs in the early stages of digitalization. Each of the two options described can be productive. However, administrations in FCS contexts tend to be faced with unique challenges relating to financing, stability, and the ability to execute long-running projects.

[1] For further information, see:
VITARA - Information Technology and Data Management (Online Course)
Use of Technology in Tax Administrations 1: Developing an Information Technology Strategic Plan (ITSP) (Technical Note)
Use of Technology in Tax Administrations 2: Core Information Technology Systems in Tax Administrations (Technical Note)
Use of Technology in Tax Administrations 3: Implementing a Commercial-Off-The-Shelf (COTS) Tax System (Technical Note)

B. An Alternate Option: Kontaktu

9. In response to a call for innovation, the IMF developed an electronic platform to support the digitalization of an FCS tax administration. When COVID-19 emerged, a request was received for digitalization support from a member country. At the time, interactions between taxpayers and the tax administration were entirely face-to-face and burdensome. Due to the pandemic, the country needed to shut down tax administration offices, and was not in a fiscal position to prioritize investments in a new tax administration IT system. The IMF and the government of pilot country agreed to develop and implement a lightweight, Minimum Viable Product (MVP) of a website for electronic filing and payment. Named Kontaktu, this innovative tool was developed and deployed entirely remotely, becoming the backbone of digital transformation in the pilot country's tax administration.

10. With successful deployment in the pilot country, the IMF subsequently approved Kontaktu for use in other FCS member tax administrations. From the outset, Kontaktu was designed for use in challenging environments. This includes scenarios where electricity and basic internet connectivity are unstable, and where IT infrastructure and financial resources are limited. Kontaktu was developed as a multi-language, open-source, and generic tool using enterprise-grade and free software. It can be hosted in commercial clouds or on government servers. Accessible through both computers and smartphones, the MVP software is delivered free of cost, with source code and manuals. With these features and successful implementation in the pilot country, Kontaktu was subsequently approved by the IMF as a resource for other FCS members facing similar challenges. Countries can adopt the entire solution or only specific modules and are free to use it as intended or modify any feature at their discretion.

11. The Kontaktu platform is considered a "digital public good." Digital public goods are open-source software, standards, models, data sets, and content that are freely accessible and designed to address key global challenges, especially in low-resource settings. They are intended to contribute to sustainable development. Various international agencies are investigating digital public goods as a possible approach to enhancing digital inclusion, particularly in emerging economies.

12. As a streamlined, accessible option, Kontaktu is useful for inexpensively iterating through development cycles. Digitalization presents an opportunity to review and modernize tax administration business processes to bring them into alignment with good international practices. As part of this, major functions and information should be reviewed (especially for registration, filing, payment, and taxpayer services). Doing so requires looking at legislation, procedures, and tax forms, among an array of other artifacts. A common mistake is digitalizing business models designed for paper-based work processes. The ability to hold the conversations needed to explore good practices, come to agreement, and then implement changes can be time-consuming and expensive, particularly if needing to engage IT suppliers. Kontaktu, because of the technology it relies on and its free software model, reduces the technological barriers that often impede progress at the early stages of digitalization.

13. Built specifically for FCS contexts, Kontaktu has features that set it apart from established options (ITAS acquisition or in-house development). Box 1 provides an overview. Annex II contains further details. Technical specifications for the platform are detailed in Annex III and the minimal hardware requirements for deploying Kontaktu server are detailed in Annex IV. Detailed security test results are included in Annex V.

Box 1. Why Kontaktu is Well-Suited for Fragile and Conflict-Affected States

- **Customizable and Flexible:** The platform is adaptable to meet country-specific requirements without needing to modify the source code. Adding new tax declarations is a simple and straightforward process.
- **Low Internet Dependency:** Taxpayers can complete all tasks offline and upload tax declarations once they have internet access.
- **Modular Design:** Implementation can be phased over time, starting with basic functionalities and gradually adding more features as needed.
- **Low Maintenance Cost:** Kontaktu can be installed on-premises or hosted using cloud providers, requiring minimal resources to operate.
- **Use of Market Standards:** Built with modern technologies such as microservices, Docker, and Java, the platform adheres to current industry standards.
- **Robust Security:** Access is controlled by user roles, and the platform employs industry-standard measures to prevent cyberattacks.
- **Software Provided Free of Cost:** The software and source code are entirely free of charge.
- **Interactive Data Analysis:** The platform includes built-in tools for generating comprehensive reports directly from the database to be used by non- IT staff.
- **Automated Data Exchange:** Tools included in the platform facilitates seamless data sharing with other departments through simple, preconfigured steps.
- **Flexibility to Adapt:** New taxes can be added without altering the platform. Machine-learning integration ensures scalability and efficiency.
- **Electronic Notifications:** Integrated modules enable automated, low-cost communication with taxpayers, reducing the need for human intervention.
- **Simplified Payment Process:** The platform supports the collection of any tax or fee within the country, streamlining payment procedures.
- **Resilience Against Failures or Attacks:** With built-in backup features, data can be securely replicated across multiple servers, including geographically separated locations, ensuring business continuity.

For further technical details, please refer to Annexes II to V.

III. Proposed Next Steps

14. The next step is to determine which option for digitalization makes the most sense in the specific country context. This could include, either: (a) acquisition of a commercial ITAS platform; (b) in-house, custom development; or, potentially, (c) implementation of Kontaktu. Because Kontaktu is provided as a digital public good (free of cost for software), it may be ideal as a transitionary measure to jump-start digitalization, after which the established options noted may be more easily pursued.

15. In all instances, the IMF is available to help navigate the options. If there is concrete interest in Kontaktu, the next step is to send a letter requesting further support. The IMF will then organize follow-up activities to help scope an implementation project. The project will include consideration for review of business processes and the actual implementation of Kontaktu, along with the technical and operational training required. The project would likely focus on a small number of taxes and taxpayers first (the large taxpayer office, for example), before pursuing wider deployment. Similarly, the IMF will remain available to help in other scenarios, where the decision is taken to acquire a commercial platform or proceed with in-house development.

16. The deployment of Kontaktu, should the country choose to proceed, will depend on the types of taxes, taxpayer segments, and modules to be adopted. The project proposal would be refined depending on the modules, number of taxes, and size and composition of the project team. During the seminar, an example of the first year was presented to give participants a general idea of what the actual project would look like. This example is reproduced below, but should be adjusted according to specific circumstances:

- A series of four to six remote preparatory meetings for the mission, during which legislation will be shared, administrative processes dissected, stakeholders identified, and the agenda discussed and adjusted.
- An Inaugural HQ mission – preferably conducted in person with an IMF team of four to six members. Logistics for this mission need to be determined, and it will conclude with a diagnostic of two or three core items for the pilot phase (e.g., registration and filing). The in-person mission option is intended to ensure synergies and alignment, with all strategic decisions made during this mission.
- Post-mission remote meetings to finalize the diagnostic and streamline the next steps.
- This HQ-mission will be complemented by remote STXs engagements – four to six engagements over the course of one year.

17. Since the General Commission of Tax in Libya is not an autonomous administration, support from the Ministry of Finance of Libya is essential for successful implementation. This backing will provide the necessary authority to promote changes and the visibility needed to drive the initiative forward. A strong commitment from political leaders underscores the project's importance and encourages collaboration among various stakeholders. Box 2 contains more detailed information about relevant drivers of success.

Box 2. Requisites for a Successful Implementation of Kontaktu

- Support from the Ministry of Finance and leadership in tax administration is the more critical factor to support the change management.
- A well-organized project requires a strong structure. Appointing a general project manager to oversee the entire initiative, along with specific submanagers for legal, core business processes, IT, and communication, ensures clear accountability and streamlined decision-making. Alongside this, a core team of dedicated professionals should be designated to coordinate efforts across departments and maintain focus on the project's goals.
- A Digitization legal framework: the legal framework should be modified to ensure the legal equivalence of paper-based and online processes.
- Effective communication is vital to gaining public trust and managing expectations. Prepare a communication campaign to explain the benefits of the modernization effort to taxpayers, employees, and other stakeholders will help to overcome cultural barriers.
- Also, there are some key decisions to be taken, such as: (i) what are the modules to be developed at the beginning; (ii) what is your appetite / capability; (iii) when is it possible to start; (iv) who will be your core team; (v) how to ensure internet availability; (vi) where to host it? In cloud or on-premises; and (vii) how many taxpayers will be in the pilot phase.

Annex I. Description of Kontaktu

Kontaktu – A Platform for Digitalization in FCS Tax Administrations

Kontaktu is a user-friendly web platform designed to support Tax Administrations in managing and streamlining their digital services. It connects key players in the tax ecosystem, including taxpayers, internal tax officers, payment authorities (like banks and mobile payment agents), customs, and treasury departments, creating a seamless and efficient workflow for all.

With Kontaktu, Tax Administrations can modernize their operations, improve taxpayer services, and simplify collaboration with other government and financial entities.

Built using reliable open-source technologies, Kontaktu is designed to be flexible, fully customizable and scalable. It can operate securely on the public Internet, whether hosted in a cloud environment or within an organization's on-premises systems.

Key **features** of Kontaktu include:

- **Versatile Modeling Tax Returns:** Kontaktu can be set up to fit the needs of tax administration with almost no need to adjust the source code.

  To achieve this objective, Kontaktu adopts an innovative strategy through which new tax declaration templates can be learned by the system, making the tax administration capable of providing self-assessment online services to taxpayers. Kontaktu employs machine learning heuristics and schemaless data storage approach capable to extract all the necessary.

  Traditionally, implementing an electronic tax returns filing system requires a specialized team of database architects, developers, and software engineers to create rigid data structures and write extensive code for validations, data transformations, and more.

  With Kontaktu's modern approach, all internal requirements can be met effortlessly. Simply provide a template file, which can be as simple as an Excel spreadsheet, and the platform automatically adapts to the underlying data structure.

- **Modern Infrastructure:** Kontaktu is built with modular components powered by reliable open-source technologies, enabling the tax administration to decide which features to enable, both for external and internal use.

  It offers a comprehensive suite of modules tailored to modern tax administration needs, including:

  - **Taxpayers Registry**: this module may be used for keeping record of taxpayers registry information, including the possibility to keep geo references and the internal relationships

between taxpayers. There is also the possibility to integrate Kontaktu with external taxpayer registry systems. It's also a possibility to make Kontaktu automatically generate new taxpayer identification numbers.

- **Filing Module**: this module is used for modeling and receiving tax returns files and other tax related forms. The taxpayers may upload their own files according to templates that are published by the tax authority. Kontaktu deals with different file formats, such as Excel spreadsheets, Word documents, PDF, and XML files. The files are transmitted online and are stored internally in a schemaless database.
- **Payments Module**: this module controls payments of taxes making use of external payment platforms such as online banking systems by means of API's.
- **Invoices Module**: this module implements 'online invoice' in different styles. It also includes additional structures for controlling the authorization of invoice issuance.
- **Communication Module**: this module implements a communication platform for different cases, such as internal communications, official reports, legislation, instructions, etc. The messages may be viewed online on Kontaktu or may be sent by e-mail or mobile app instant messages.
- **Tax Domicile Module**: this module implements the concept of an 'Electronic Tax Domicile', which may be useful for delivering tax notifications to taxpayers with awareness deadline control.
- **Tax Credit and Previous Loss Module**: this module includes features related to tax credit balance control, tax credit claims and previous loss control accounted in tax returns to be used with debt compensations.
- **Export Module**: this module implements a supply chain management for export operations, including stock control of goods to be exported.
- **Integration Agents Module**: this module makes use of a distributed net of 'integration agents', useful for IoT (Internet of Things) and also for integrating databases and services from different government agencies.

- **Scalability and Security:** Kontaktu delivers exceptional performance thanks to its advanced design. Its robust architecture supports horizontal scalability and adapts to flexible data structures, ensuring reliability even as demands grow.

  The data is internally stored using No-SQL data storage, including replication and sharding capabilities.

  Built with security in mind, Kontaktu complies with industry standards and incorporates multiple layers of protection to safeguard your data and operations.

  For example, Kontaktu includes these security measures:

  - **Compliant encryption policy**: The system follows good security practices regarding the configuration and use of digital certificates for encryption of the communication channel, ensuring the use of current encryption algorithms.
  - **Container isolation**: Following a containerized architecture, each internal component only connects to the intended interfaces.

- **Automatic blocking for suspected intrusion attempts**: The entry point of the architecture actively monitors unsuccessful login attempts, enabling automatic blocking of suspicious sources.
- **Backup strategy**: With Kontaktu there is a built-in capability to replicate and keep synchronized one or more replicas of the entire system, which in turn may reside in an entirely different location.
- **Security measures in both back and front ends**: Several security measures are considered in the development of both back and front ends, such as: strict Content Security Policies, Cross-Site Request Forgery tokens, configurable privileges and user profiles related to Rule Based Access Control conforming to the principle of least privilege, adoption of open standards (OpenId/OAUTH) for user authentication using pluggable identity providers, adoption of strong password policies, rate limiting by means of reCAPTCHA protection, enforcement of TLS/SSL both externally and internally, validation and treatment of user input in order to prevent XSS and other injection attacks.
- **Logging system**: The users activity are registered and logged in the system, which may be later queried by the IT teams in order to spot suspicious events.

- **Technological Autonomy for the Business Area:** Kontaktu empowers business teams to take control, enabling them to design and implement strategic decisions directly, without relying on IT support. This streamlined approach ensures faster decision-making and greater flexibility for your organization.

  A data analysis tool was entirely developed in Kontaktu and is meant to be as simple as possible, to be easily understood and operated by non-IT specialists, such as the business level teams, but to still enable them to perform data cross matching with multiple sources of data.

  It enables any kind of data to be matched, such as: VAT and CIT returns, taxpayers registry, customs data, electronic invoices, tax payments, payroll, real estate and IoT collected data.

  It's also possible to build dashboards with different types of charts for assisting business intelligence tasks and also provides maps which may include geo located data related to the taxpayers.

Annex II. Technical Specifications of Kontaktu

Programming language	**Java (backend)** **Javascript, CSS, HTML (frontend)** **Groovy (scripts)**
Programming Framework and Libraries	**Spring / SpringBoot** **Thymeleaf** **JQuery** **Semantic UI** **Tabulator JS** **Codemirror** **ToastUI**
Internal Database	**ElasticSearch (with multiple data nodes)**
Reverse Proxy	**NGINX**
Digital Certificate Provider	**Lets Encrypt**
Container Orchestration	**Docker Compose (also possible to use with Kubernetes)**
Dashboards	**Kibana**
Development Tools	**Maven** **Eclipse** **GIT**
Supported Input File Formats	**Excel (XLS, XLSX, XLSM)** **Word (DOC, DOCX)** **PDF (including forms)** **CSV** **XML** **JSON**
Supported Databases (for data exchange)	**SQL Server** **My SQL** **Oracle Database** **Postgre** **Firebird**

Annex III. Minimal Hardware Requirements

Kontaktu may be deployed in a cluster with multiple hosts, in the cloud or on-prem.

The simplest and easiest configuration of Kontaktu deployment consists of one single server with the following characteristics:

- RAM Memory: 32 GB
- CPU: 4 cores x86_64
- Disk: 60 GB SSD
- OS: Linux 64 bits (RedHat, CentOS or similar)
- Connectivity to the Internet and accessible externally by port 443 (SSL)
- Any public external domain name to be assigned to Kontaktu server.

Annex IV. Security Report

12/4/24, 2:22 PM SSL Server Test: kontaktu.myvnc.com (Powered by Qualys SSL Labs)

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > kontaktu.myvnc.com

SSL Report: kontaktu.myvnc.com (44.208.235.218)

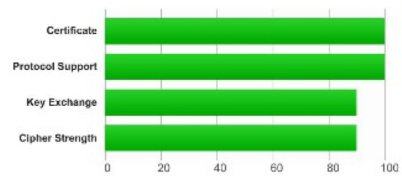
Assessed on: Tue, 03 Dec 2024 12:13:33 UTC | HIDDEN | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Certificate #1: EC 256 bits (SHA384withECDSA)

Server Key and Certificate #1

Subject	kontaktu.myvnc.com Fingerprint SHA256: bfe10effab81859f11b9a5c96233dc68d3763f93579ca4526fb8937cbde96317 Pin SHA256: XAOSHehAmJocKDoApRDcvdtkeVaDlyWCJtE8zQ/Ygg=
Common names	kontaktu.myvnc.com
Alternative names	kontaktu.myvnc.com
Serial Number	04a5c967003d9a3f237de40dc290bbc004c9
Valid from	Sun, 10 Nov 2024 14:26:24 UTC
Valid until	Sat, 08 Feb 2025 14:26:23 UTC (expires in 2 months and 5 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	E5 AIA: http://e5.i.lencr.org/
Signature algorithm	SHA384withECDSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://e5.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	2 (2022 bytes)
Chain issues	None

#2

https://www.ssllabs.com/ssltest/analyze.html?d=kontaktu.myvnc.com&hideResults=on 1/4

Additional Certificates (if supplied)

Subject	E6 Fingerprint SHA256: 5cfdb3cf31b28f23d87c0f3a0ce642f64069a9fb7cfe28270bb5dc0f1e16ab Pin SHA256: NYbU7PBwV4y9J87c4guWTd8FJ+uudrXL0s4V4aRcg=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 2 years and 3 months)
Key	EC 384 bits
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Cipher Suites

 # TLS 1.3 (server has no preference)

TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256

 # TLS 1.2 (server has no preference)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH secp521r1 (eq. 15360 bits RSA) FS	256

Handshake Simulation

Android 4.4.2	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Android 5.0.0	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp521r1 FS
Android 6.0	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.0	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
BingPreview Jan 2015	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
Chrome 49 / XP SP3	Server sent fatal alert: handshake_failure		
Chrome 69 / Win 7 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Googlebot Feb 2018	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS

Handshake Simulation

IE 11 / Win 7 R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
IE 11 / Win 8.1 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
IE 11 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Edge 15 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 16 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 18 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
Edge 13 / Win Phone 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 8u161	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.1l R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS
OpenSSL 1.0.2s R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.1.0k R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure		
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure		
Safari 7 / OS X 10.9 R	Server sent fatal alert: handshake_failure		
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure		
Safari 8 / OS X 10.10 R	Server sent fatal alert: handshake_failure		
Safari 9 / iOS 9 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / iOS 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Apple ATS 9 / iOS 9 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp384r1 FS
YandexBot Jan 2015	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp521r1 FS

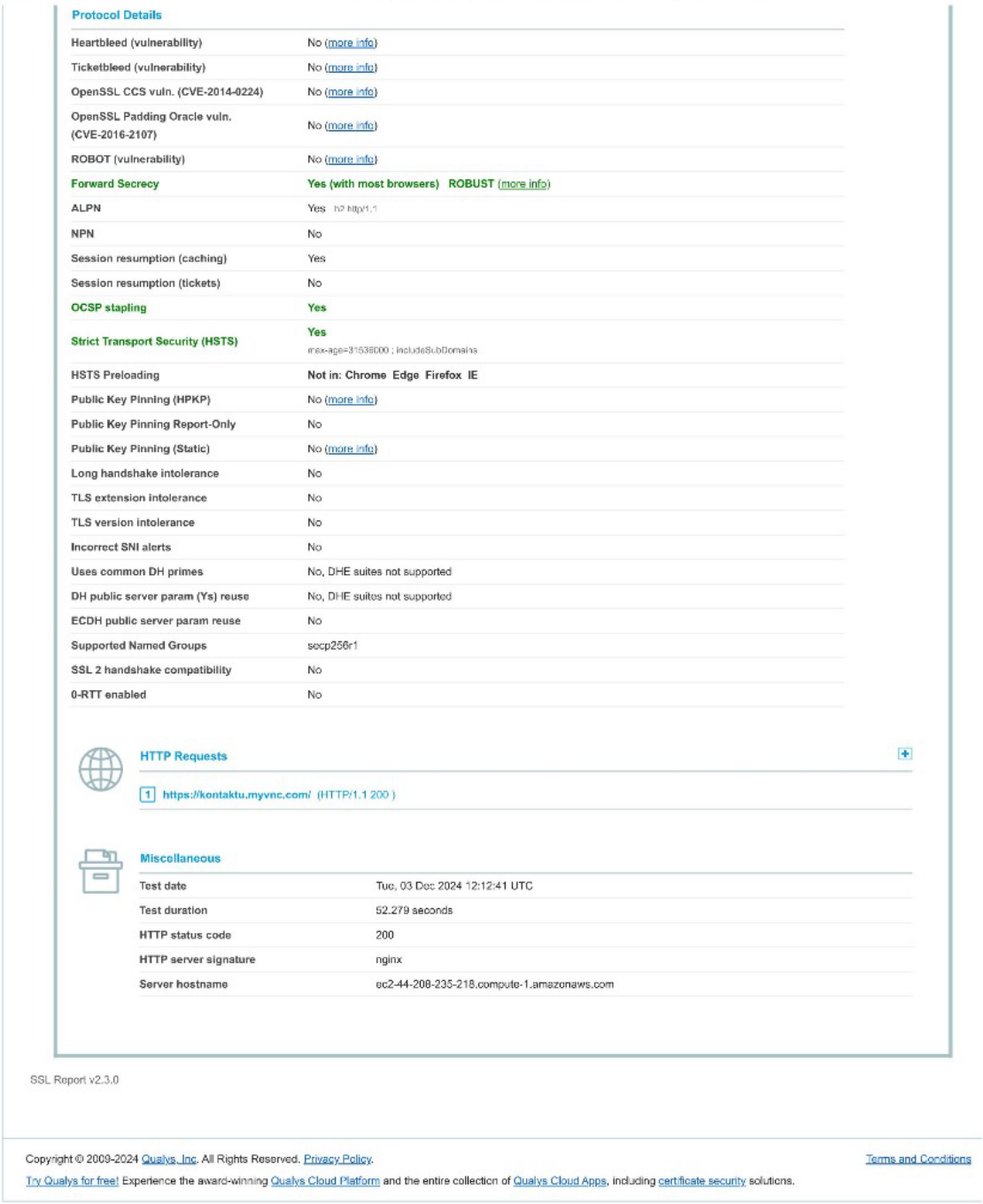
 # Not simulated clients (Protocol mismatch)

Click here to expand

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.
(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.
(R) Denotes a reference browser or client, with which we expect better effective security.
(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).
(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No



Protocol Details

Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes h2 http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	Yes
Strict Transport Security (HSTS)	Yes max-age=31536000 ; includeSubDomains
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	secp256r1
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 https://kontaktu.myvnc.com/ (HTTP/1.1 200)

Miscellaneous

Test date	Tue, 03 Dec 2024 12:12:41 UTC
Test duration	52.279 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	ec2-44-208-235-218.compute-1.amazonaws.com

SSL Report v2.3.0

Copyright © 2009-2024 Qualys, Inc. All Rights Reserved. Privacy Policy. Terms and Conditions

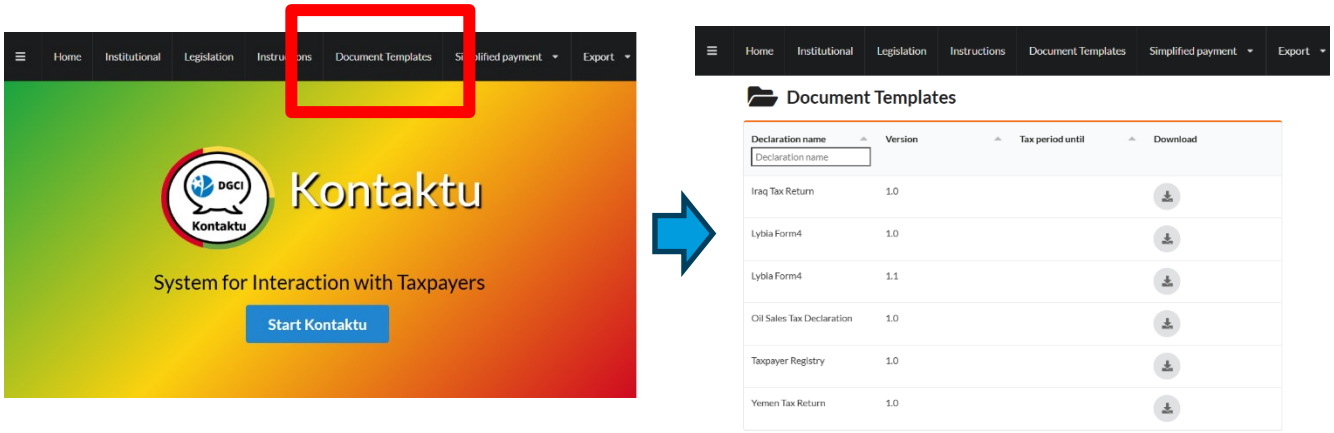
Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.

Annex V. Taxpayer Experience

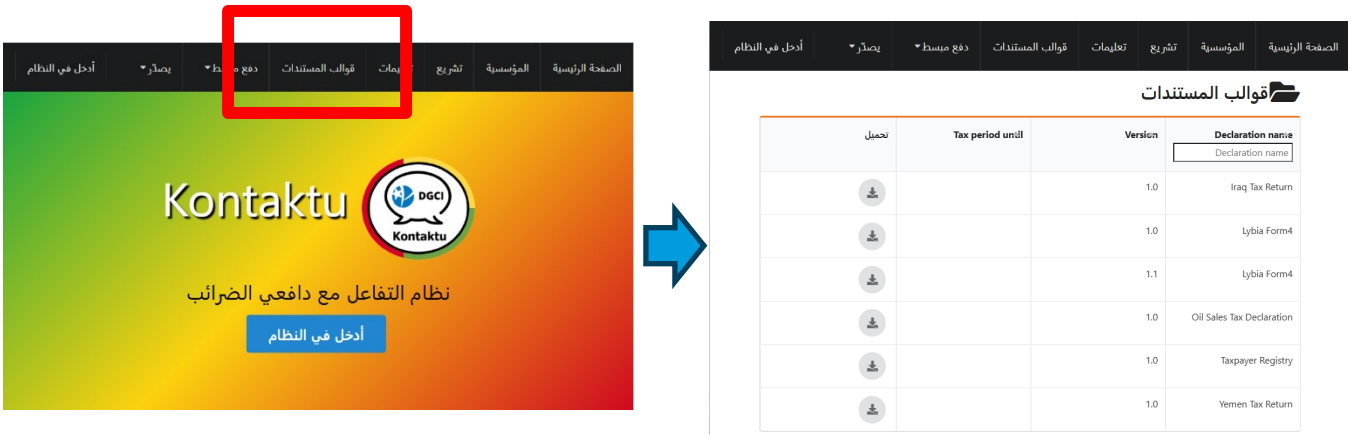
From the taxpayers' point of view, the experience for filing tax returns is as simple as follows:

1. **Download the template for the tax return**. The taxpayer will first access the Kontaktu server using the public Internet Address defined by the Tax Administration and will locate the template for the specific tax return he wants to submit. This takes just two clicks in the web user interface. He file may be in any of the file formats as pre defined by the tax authority to allow electronic filing (without the need for a paper printed version): Excel spreadsheet, Word document, PDF (including forms).

- English version:



- Arabic version:



2. **Fill in the fields**. The taxpayer will fill in all the required fields that has been defined by the tax authority in the template. Usually, it will be a protected file, allowing only some parts of it to be

changed by the taxpayer, and including local validations (for example, preventing the taxpayer from typing texts where dates or numbers are expected). If it's an Excel spreadsheet, it may also include pre-defined formulas, programmed by the tax administration, in order to do all the calculations (e.g. for summing the incomes, subtracting the expenses and applying the tax rate in order to compute e display the amount due). Taxpayer may take his time to fill in all the required fields in all tables regardless of Internet connectivity (no Internet connection is needed for this task).

- Template (empty file with the layout pre-defined by the Tax Administration):

الجدول (ب)

بيان الإيرادات خلال السنة

رقم مسلسل	جملة الإيرادات	درهم	دينار	نسبة الربح الأجمالي	الربح الأجمالي	
					درهم	دينار
.1	إيراد التجارة				0	0
.2	إيراد الصناعة				0	0
.3	إيراد الحرفة				0	0
.4	إيرادات العمليات العارضة				0	0
	إجمالي الربح خلال السنة الضريبية				0	0

بيان بالربح الخاضع للضريبة

رقم مسلسل	البيان	القيمة	
		درهم	دينار
	الربح الإجمالي وفقاً للجدول (ب)	0	0
	تخصم المصروفات الإدارية والعمومية والخسائر المرحلة:-		
.1	الأجور والمرتبات		
.2	حصة الممول في الضمان الإجتماعي		

- File filled in by the taxpayer

الجدول (ب)

بيان الإيرادات خلال السنة

رقم مسلسل	جملة الإيرادات	درهم	دينار	نسبة الربح الأجمالي	الربح الأجمالي	
					درهم	دينار
.1	إيراد التجارة	1000	1000	80,00%	800	800
.2	إيراد الصناعة	200	200	50,00%	100	100
.3	إيراد الحرفة	300	300	80,00%	240	240
.4	إيرادات العمليات العارضة	400	400	70,00%	280	280
	إجمالي الربح خلال السنة الضريبية				1420	1420

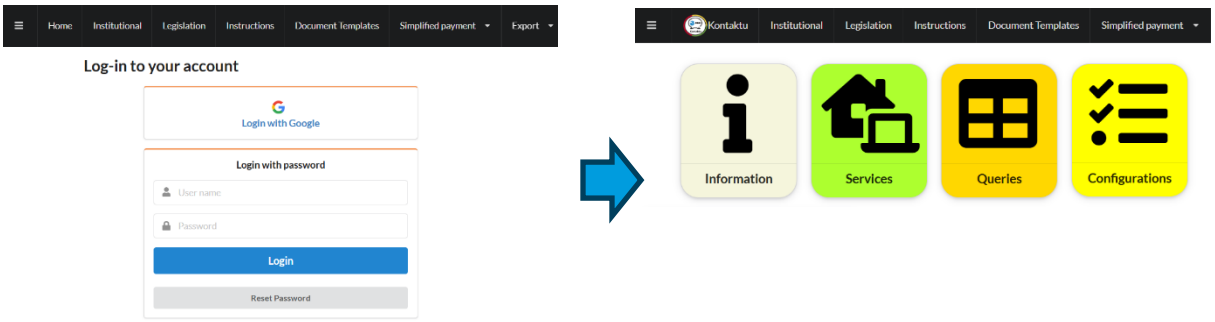
بيان بالربح الخاضع للضريبة

رقم مسلسل	البيان	القيمة	
		درهم	دينار
	الربح الإجمالي وفقاً للجدول (ب)	1420	1420
	تخصم المصروفات الإدارية والعمومية والخسائر المرحلة:-	200	200
.1	الأجور والمرتبات	100	100
.2	حصة الممول في الضمان الإجتماعي	150	150

3. **Taxpayer logs into Kontaktu.** After the taxpayer has finished filling all the required information in the tax return, he logs in the Kontaktu server using the user account that has been already provided by the Tax Administration. The Kontaktu server may offer different login options according to how the Tax Administration has configured it.

   In order to proceed, this user account must have been previously assigned to a taxpayer identification number related to the company (e.g. may be an accountant, a director or a legal representative of the company about which the tax return is related to). Kontaktu enforces these rules in order to prevent unauthorized personnel from submitting files on behalf of others.

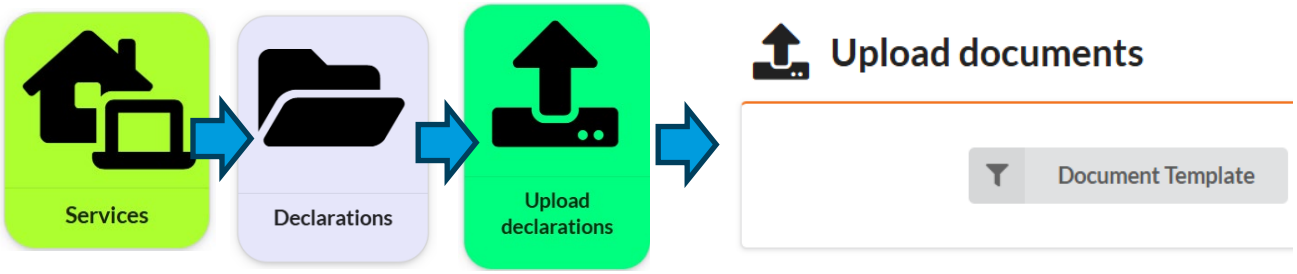
- English version:



- Arabic version:

4. **Taxpayer uploads the file.** It takes just 2 clicks to get to the screen where the taxpayer will be able to upload his tax return. By the time he submits his file, Kontaktu will perform all the data validations. In case of errors, missing data or unauthorized access, the file is rejected and the taxpayer receives a warning message. Otherwise, he receives a successful confirmation, and all the related tax payment slips are automatically generated and available to him.

- English version:



- Arabic version: