TENDER NOTICE

EA/02-66-2022

E-Signature Solution

1. Sealed Bids are invited from registered Companies for Provisioning of E-Signature Solution**.** The Hard Bid Documents are also available in Etisalat head office and can be obtained from procurement department as well can download it from Etisalat Afghanistan website (www.etisalat.af, Tenders).

2. Bids shall be sent via email to snabizada@etisalat.af **Deadline: 26-December-2022**

3. Bids received after the above deadline shall not be accepted.

Note: If you submit your commercial part of proposal by email, please provide it in **password protected document/format**. We will request the password once here the concerned committee started the bid's commercial evaluation.

4. The bidders should have similar experience in this project.

5. Bidders should be registered with Etisalat Afghanistan in Vendor Registration List. If any interested bidder is not registered, first they should register their company before tender deadline and submission of bid.

6. Etisalat Afghanistan reserves the right to accept or reject any or all bids and to annul the bidding process at any time, without thereby incurring any liability to the affected bidder(s) or any obligations to inform the affected bidder(s) of the grounds for Etisalat Afghanistan action.

7. All correspondence on the subject may address to Shoaib Nabizada, Sr. Analyst Procurement & Contracts, Etisalat Afghanistan. Email snabizada@etisalat.af and Phone No.+93781 204113 .

Ihsanullah Zirak
Director Procurement & Contracts
Ihsan Plaza, Shar-e-Naw, Kabul, Etisalat Afghanistan
E-mail**:** ihsanullah@etisalat.af

Request for Proposal

(RFP)

For

E-Signature Solution

1. DEFINITIONS

In this document, the following terms and meanings shall be interpreted as indicated:

1.1 Terms.

"Acceptance Test(s) "means the test(s) specified in the Technical Specifications to be carried out to ascertain whether the Goods, Equipment, System, Material, Items or a specified part thereof is able to attain the Performance Level specified in the Technical Specifications in accordance with the provisions of the Contract.

"Acceptance Test Procedures" means test procedures specified in the technical specifications and/or by the supplier and approved by EA as it is or with modifications.

"Approved" or "approval" means approved in writing.

"BoQ " stands for Bill of Quantities of each job/work as mentioned in this contract and its annexes according to which the contractor shall supply equipment & services and subject to change by agreement of both parties.

"Bidding" means a formal procurement procedure under which sealed bids are invited, received, opened, examined and evaluated for the purpose of awarding a contract.

"Bid/Tender Document" means the Bid/Tender documents issued by EA for invitation of Bids/Offers along with subsequent amendments and clarifications.
"CIF" means "Cost Insurance Freight" as specified in INCOTERM 2010.

"Competent Authority" means the staff or functionary authorized by EA to deal finally with the matter in issue.

"Completion Date" means the date by which the Contractor is required to complete the Contract.

"Country of Origin" means the countries and territories eligible under the rules elaborated in the "Instruction to Bidders ".

"Contract" means the Contract between Etisalat Afghanistan (EA) and the Contractor and comprising documents.

"Contractor" means the individual or firm(s) ultimately responsible for supplying all the Goods/Equipment/Systems/Material/Items on time and to cost under this contract to EA.

"Contractor's Representative" means the person nominated by the contractor and named

as such in the contract and approved by EA in the manner provided in the contract.

"Contract Documents" means the documents listed in Article (Contract Documents) of the Form of Contract (including any amendments thereto) or in any other article in this contract.

"Contract Price" means the price payable to the Contractor under the Contract for the full and proper performance of its contractual obligations.

"Day" means calendar day of the Gregorian calendar.

"Delivery charges" means local transportation, handling, insurance and other charges incidental to the delivery of Goods to their final destination.

"D.D.P" means Delivered Duty Paid as defined in the Incoterms 2010 including the unloading responsibility of bidder/seller.

"Effective Date" means the date the Contract shall take effect as mentioned in the Contract.

"Etisalat Afghanistan (EA)" means the company registered under the Laws of Islamic republic of Afghanistan and having office at Ihsan Plaza Charahi Shaheed Kabul in person or any person dully authorised by it for the specific purpose for the specific task within the Contract and notified to contractor in writing.

"Final Acceptance Certificate" means the certificate issued by EA after successful completion of warranty and removal of defects as intimated by EA.

"Force Majeure" means Acts of God, Government restrictions, financial hardships, war and hostilities, invasion, act of foreign enemies, rebellion, revolution, riot, industrial disputes, commotion, natural disasters and other similar risks that are outside of Contractor's and EA's control.

"Goods Receipt Certificate" means certificate issued by the consignee certifying receipt of Goods in good order and condition.

"Liquidated Damages" mean the monetary damages imposed upon the contractor and the money payable to EA by the contractor on account of late delivery of the whole or part of the Goods.

"**L.o.A**" means Letter of Award issued by EA to successful bidder with regard to the award of tender.

"Month" means calendar month of the Gregorian calendar.

"Offer" means the quotation/bid and all subsequent clarifications submitted by the Bidder and accepted by EA in response to and in relation with the Bid Documents.

"Origin" means the place where the Goods are mined, grown or produced from which the ancillary services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembling of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components.

"EA's Representative" shall mean the representative to be appointed by EA to act for and on behalf of EA with respect to this Contract.

"Specifications" means the specifications, provided in the Contract and its annexure and in EA Tender Specifications and where the Contract is silent and in cases of conflicting specifications appearing in the documents, based on the latest version of ITU-T recommendations.

"Supplier/Vendor" (used interchangeably) means the individual or firm ultimately responsible for supplying all the Goods on time and to cost under this Contract acting individually alone or as a "prime contractor" for a consortium.

"Supplier's Representative" means the person nominated by the Contractor and named as such in the Contract and approved by EA in the manner provided in the Contract.

"Warranty Period" shall mean the period of 12 months or any extended period starting from the acceptance of the delivered Goods in good order and conditions at consignee's certified by EA authorized representative (s).

"**Cybersecurity Terms**" **Annexure B**

2. INTRODUCTION TO WORK.

2.1 Bids are invited for provision of E-Signature Solution in accordance with Etisalat specifications as per **Annexure A.**

3. Validity of Offers

The Tenders must be valid for a minimum of 90 days from the Tender closing date, or as may be specified by Purchaser in the Tender documents.

4. Price

4.1 International Bidders can quote CIP Kabul and Local Bidders shall quote DDP Kabul prices accordingly.
4.2 DDP Prices shall be inclusive of Custom Duties and all Taxes as applicable in Afghanistan as per Islamic Republic of Afghanistan Tax Laws.
4.3 CIP prices shall be quoted in USD and DDP in Afghani currency only.

5. Payment Terms.

5.1 EA will make payment equal to **75%** of the amount after Ready for Service (RFS).
5.2 Balance **25%** of the amount after issuance of Provisioning Acceptance Certificate (PAC).
5.3 EA will make payment for Maintenance/Support on quarterly in arrears.
5.4 Payment shall be made by bank transfer after receipt of original Hardcopy of invoice.
5.5 No advance payment to contractor.
5.6 EA shall make prompt payment, within thirty days of submission of an invoice/claim by the contractor subject to availability of pre requisite documents specified under the contract and adjustment of penalty (if any) on account of late delivery and/or defective Goods replacement after confirmation from Project Director.
5.7 Payments are subject to deduction of income tax at prevalent rate from the relevant invoices of the contractor and paid to the Tax Authorities, except those especially exempted by the authorities. EA will issue certificate of deductions to the contractor to enable him to settle tax returns with the concerned authorities.

6. Penalty:

6.1 If the contractor fails to complete the said job on or before the Completion Date, the Contractor shall pay to the Purchaser as and by way of Penalty resulting from the delay, the aggregate sum of one percent (1%) of Total Contract price of the delayed services for each week and pro-rata for parts of week, for delay beyond the specified date, subject to a maximum of ten percent (10%) of the Total Contract Price of the service(s). In the event that delay is only in respect of small items which do not affect

the effective utilization of the system, penalty shall be chargeable only on the value of such delayed items.

6.2 Any penalty chargeable to the Contractor shall be deducted from the invoice amounts submitted by the Contractor for payment, without prejudice to the Purchaser's rights

7. Construction of Contract:

The Contract shall he deemed to have been concluded in the Islamic Republic of Afghanistan and shall be governed by and construed in accordance with Islamic Republic Afghanistan Law.

8. Termination of the Contract

8.1 If during the course of the Contract, the Contractor shall be in breach of the Contract and the Purchaser shall so inform the Contractor by notice in writing, and should the breach continue for more than seven days (or such longer period as may be specified by the Purchaser) after such notice then the Purchaser may immediately terminate the Contract by notice in writing to the Contractor.

8.2 Upon termination of the Contract the Purchaser may at his option continue work either by himself or by sub-contracting to a third party. The Contractor shall if so required by the Purchaser within 14 days of the date of termination assign to the Purchaser without payment the benefit to any agreement for services and/or the execution of any work for the purposes of this Contract. In the event of the services/jobs being completed and ready for utilization by the Purchaser or a third party and the total cost incurred by the Purchaser in so completing the required services/jobs being greater than which would have been incurred had the Contract not been terminated then the Contractor shall pay such excess to the Purchaser.

8.3 The Contractor shall not have the right to terminate or abandon the Contract except for reasons of force majeure.

9. Local Taxes, Dues and Levies:

9.1 The Contractor shall be responsible for all government related taxes, dues and levies, including personal income tax, which may be payable in the Afghanistan or elsewhere.

9.2 Withholding tax (if applicable) shall be deducted on local portion only as per prevailing rates as notified Islamic republic of Afghanistan. The amount of withholding Tax(s) is 2% of all project cost for local/registered companies who have Afghanistan Government Official Work License and 7% for International/ nonregistered companies.

9.3 The contractor will fully inform itself of all Islamic Republic of Afghanistan Tax Regulation and will pay all taxes; duties, tariffs and impositions lawfully assessed against the contractor for execution and performance of the contract.

Annexure-A

Objective:

It is required that a Service Provider be appointed to supply; implement; support and maintain a digital signature solution to enable the reviewing, tracking, exchange files for signing electronic documents. The solution will enable online signing and reduce the need for physical sign-off of documents. This is particularly important for Executives, Group Managers, Senior Managers, Managers and Supervisors who are not
always physically present to sign-off documents. The solution will aid efficiency as approvals can be done remotely via this digital signature solution. It will further limit the use of paper and is a key step on the journey to a paperless and digitized EA. This will improve the approval process by eliminating the need to print, sign and scan documents. It will further improve the tracking process and audit trails. The service provider is required to supply the digital software, implement it, host the service.

SOW for E-Sign Solution:

1. Solution should be able to provide digital signature capability for the documents (Word Documents, Excel Sheets, PDF Files, Scanned Files) within SharePoint, One Drive, MS Teams and as a stand-alone (on laptops etc) and the initiator should be able to view the status of documents.
2. Initiator should be able to build a workflow and to set the signer(s) and the signing order using their email address and should be able to use a pre-defined workflow template pre-set by system admin.
3. It should provide functionality to add the names, SharePoint groups (integrate with AD, office365, Sales Force, Microsoft SharePoint, Adobe Reader, Ms. Word , Ms outlook, Ms. Teams, Ms. Teams Approval App Power Automate and Power Apps, etc.)
4. Support the following Internet Browsers on desktop and mobile: IE, Chrome, Edge, Edge Chromium, Firefox, and Safari.
   and email addresses of the individuals (recipients) who needs to sign the document and provide an option to specify the order of signing and re-assignment option.
5. The solution should provide sufficient security and advanced authentication methods (2 factor authentication) to validate the signatory's identity and the data should be securely

encrypted. And no one should be able to modify/changes the signatures or document and it should be detected by the provided solution.

6. build the template of elements needed for the signature, such as (Display Name, Initials, Email Add, Signature, Stamp and Date & Time.
7. The signature of any user can be set using any of these methods (Choose, Draw, Upload Scanned Signature Image) and signatures should be visible on print out to papers if that is required for any purpose.
8. Using DSA algorithm with asymmetric cryptography (minimum key length shall be 1024) is a must.
9. The solution should have functionality of data availability as backup in its storage.
10. The system can work on multiple device types; mobiles, laptops, tablets with different platforms; Windows, MAC, iOS, and Android.
11. The documents put through the digital signature solution workflow must always be secured. They must only be viewable by parties who are meant to view them.
12. With the implementation of the digital signature solution, EA's data classification policy must be considered.
13. Third party (external) users can be part of the signing workflow.
14. All Security measures apply for both ETISALAT AFGHANISTAN and third party (external) users of the system.
15. Third Party (External) users do not need to be customers of the same e-signature system service provider.
16. The system allows for any user to setup a signing delegate when an important document needs to be signed and the signing party is away. The workflow should be able to handle this.
17. The signature should be independently verifiable, without relying on the electronic signature service or website to be validated.
18. The solution should provide the feature to convert the document to Word, PDF, JPEG And much more document/image types. Signed documents can be exported for archival outside the system manually and using integration with SharePoint Online.
19. Feel confident knowing that your digitally signed document is tamper proof and protected from improper access and use, is verifiable and defensible, and includes audit details proving accurate signing actions; all details that judges will look for when determining document legality.
20. The Solution should provide locking the signature of approver/signer.

Implementation and Configuration:

1. End user Training
2. Admin training
3. SSO Configuration
4. Configuration for SharePoint Out-of-the-Box Integration, MS Office 365 + Teams Configuration.
5. Configuration for MS Dynamics 365 Out-of-the-Box Integration.
6. Workflow + Templates Creation

License Requirement:

1. Solution should have cloud & On Prem-based subscriptions

2. Solution should have available licensing schemes, per user, per document, etc.

3. Solution should Provide the cost per different license schemes.

4. ETISALAT AFGHANISTAN can decide on the best licensing scheme to fit needs for 20 to 30K transactions per year or license for 700 users.

The license type should have all the above features and license should be dynamic and can be easily reassigned or replace a license holder with another one.

Vendor Requirements:

1. Service provider is reputable and can provide evidence of service being used by other clients in any region.
2. Complies with Standards for the European Union; eIDAS.
3. Complies with Standards in the United States: complies with the definition of an electronic signature under the Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA)
4. Complies with International standards for electronic signature.

Integration Requirements:

The solution should be able to integrate with Ms SharePoint (all versions), Azure AD, office365, Sales Force, Adobe Reader, Ms. Word , Ms outlook, Ms. Teams, Ms. Teams Approval App Power Automate and Power Apps, etc). It should be able to send the document link (one document to multiple recipients) via email to the individuals (recipients) who need to sign. Once the document is complete and signed, it should be stored securely for easy retrieval.

Security Requirements:

The Service Provider will be expected to comply with EA networks and information security standards. EA reserves the right to audit the environment where the solution will be hosted the
cost of which will be incurred by EA.
Furthermore, the solution shall use DSA algorithm with asymmetric cryptography (minimum key length shall be 1024).

AUDITING:

Knowing exactly where your documents are and where they've been is a crucial component of security and compliance. The solution should provide detailed auditing reports and features so customers can stay informed about their document workflows.

Detailed audit trails track each document by IP address and timestamp, so you have full knowledge of where, when, and who is always viewing your documents.

Certificate of completion provided for every document with the associated IP address, email address, timestamp, and name of signer.

Track the deletion of documents and folders, modified parts and each step of the way. The delete folder/option history should allow us to see where, when, and by whom any folder/item was deleted,

The solution guarantees non-repudiation; a signing party cannot deny having signed any document; they cannot say "That is not my signature! " modified, and edited. (Need audit log/trail for all trach changes in DOCs).

Solution should guarantee integrity against man in the middle attacks. The user can verify the service provider has sent the file and that it has not changed by anyone in the middle.

Solution should provide detailed login and audit trail accessible by system admins. Each signed document must be backed by an audit trail that captures intent to sign for each individual signature and provides granular, consistent, timestamped evidence as to every step in the entire signature process.

Support:

24/7 support is required in case of any issue/incident, or any information required to be delivered to end user, remote support should be considered in below ways.

1- 24/7 support by call.
2- Taking remote session if the issue not resolved by phone
3- SLA to be implemented in support cases.

Annexure - B

Important Note:

Bidders, vendors, and any concerned party shall fill all the fields in the below table, any missing or non-compliant item may cause disqualifying the proposed system from the Etisalat Security side.

No.	Description	Compliance (YES/NO/NA)	Comments
1	**Etisalat Security Requirements**		
1.1	The Contractor/Supplier/vendor to sign Non-Disclosure Agreement (NDA) with Etisalat before finalizing RFx/contract/POC agreement as per Etisalat NDA process.		
1.2	Contractor/Supplier/vendor equipment's (e.g. Servers, PCs, etc.) that are connected to Etisalat network must be securely wiped before taking out of Etisalat premises.		
1.3	The proposed/contracted system shall pass Etisalat Security Audit (Vulnerability Assessment/Penetration Testing) before go-live/service acceptance by Etisalat. Contractor/Supplier/vendor shall provide SLA for fixing Security gaps based on severity.		
1.4	Contractor/Supplier/vendor shall fix all security issues identified and reported by ETISALAT and/or Third Party Contracted to do the testing, with no additional cost		
1.5	Contractor/Supplier/vendor confirms that its products/solution are tested for weaknesses via methods such as Vulnerability Assessment, penetration testing, red teaming exercises and scans that check for compliance against the baseline security standards or security best practices, before the new product or any of its releases is delivered to ETISALAT. The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the proposed solution.		
2	**Security Architecture**		
2.1	The Contractor/Supplier/vendor shall ensure that proposed solution shall comply with the applicable IT and Telecom Security standards (such as Afg. NESA (SIA) IA V2, Afg. DESC (ISR), Afg. TRA, 3GPP, ETSI, ENISA, CSA, NIST, PCI, ISO, GDPR etc.) The Contractor/Supplier/vendor shall confirm the applicable standard.		
2.2	The proposed solution shall support the latest operating systems and application versions. Contractor/Supplier/vendor to ensure proposed solutions will run the latest stable software, operating system, and firmware.		
2.3	The solution shall be designed with multi-tier architecture, (Demilitarized Zone (DMZ), middleware, and private network). Any system accessible from the Internet shall be on the DMZ and access to internal sensitive data shall be secured through the middle tier		

No.	Description	Compliance (YES/NO/NA)	Comments
	application proxy.		
2.4	The proposed solution shall not impact or relax existing Etisalat security control or posture.		
2.5	The performance of the proposed system shall meet the business requirements without disabling or removing any existing security control		
2.6	The Contractor/Supplier/vendor shall provide only secure methods of communication such as HTTPS, SFTP, SCP, TLS1.3, IPSEC, SRTP, SSH v2, SNMPv3 between the proposed nodes. Non-secure protocols such as Telnet, HTTP and FTP shall not be used.		
3	**Password Security**		
3.1	All Operating Systems (e.g. Linux and Windows) shall be hardened according to well-known standards such as, but not limited to NIST, CIS security benchmark, and NSA.		
3.2	The proposed system includes password management module that supports the following features:		
3.3	Setting the minimum password length		
3.4	Password complexity, and not accepting blank passwords		
3.5	Maximum password age and password history		
3.6	Account lockout		
3.7	Enforce changing password after first login		
3.8	Prompt / notify for the old password on password changes		
3.9	The password shall be saved in hashed format (i.e. irreversible encryption)		
3.10	Forgetting or resetting password function shall support using OTP or email for verification		
4	**Authentication**		
4.1	The proposed system shall not provide access without valid username and password.		
4.2	All user access to the proposed system shall support Privilege account Management (PAM) integration.		
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent password dictionary attacks		
4.4	For mobile applications, the proposed system shall support and uses fingerprint authentication method		
4.5	The proposed system supports and uses secure authentication protocols, like Kerberos, LDAP-S, NTLM V2 and above, HTTPs (for web applications)		
4.6	The proposed system will not use insecure authentication protocols, like NTLM v1, HTTP (for web applications)		
4.7	The proposed system shall support session timeout settings		

No.	Description	Compliance (YES/NO/NA)	Comments
4.8	The proposed solution shall support secure API architecture to integrate systems to exchange data where deemed necessary.		
5	**Authorization**		
5.1	The proposed solution shall support role-based access controls that includes access profiles or security matrix (i.e. Role Name VS. Access Permissions)		
5.2	The proposed system supports role-based access permissions, i.e. Administrator, Operator, Viewer, User…		
6	**Software Security**		
6.1	The software development and testing will not run on the production systems, and will be running in an isolated environment		
6.2	The software source code will not include clear-text passwords		
6.3	The software code will not include insecure protocols, like FTP, telnet ...etc.		
6.4	The software testing will not use live/production sensitive or PII data unless it's masked as Etisalat security policy		
6.5	The proposed system enforces input and output validation to prevent security attacks, like SQL Injection, Buffer Overflow…etc.		
6.6	For web portals, the proposed system includes all security controls to prevent / protect from OWASP Top 10 security attacks and risks		
6.7	For mobile application, the proposed system shall include security checks / controls to protect from mobile attacks, like SSL Pinning, Jailbreak, Anti-debug, Anti-hooking, and Advanced Obfuscation…		

No.	Description	Compliance (YES/NO/NA)	Comments
7	**Security Event Logging**		
7.1	Proposed systems shall support standard logging protocols such as CIFS/Syslog/CSV logs files		
7.2	The system shall generate and support audit logs that contain the following fields (as a minimum): a) Username b) Timestamp (Date & Time). c) Client IP Address d) Transaction ID & session information		
7.3	The proposed solution shall support the integration with Etisalat NTP for time synchronization and accurate logging.		
8	**Public Cloud Security**		
8.1	Etisalat customers' and staff personal data (PII: name, contacts, address, Emirates ID, Passport number, Nationality …) is encrypted at rest and in transit using a strong industry-standard encryption protocol		
8.2	The Public Cloud setup that stores PII information shall be hosted in the Afghanistan		
8.3	The Public Cloud setup is hosted in a dedicated tenant for Etisalat (i.e. not shared)		
8.4	The Public Cloud data center shall not be moved to another country or location without prior coordination and approval from Etisalat		
8.5	All Etisalat data will be permanently erased from the Public Cloud on termination of the service or support agreement		
8.6	The proposed Cloud system supports Etisalat Cloud Access Security Broker (such as Microsoft MCAS, Netskope CASB)		
9	**Virtualization and Container Security**		
9.1	If applicable, Bidder shall ensure the proposed virtualized infrastructure, service based and micro services architecture to support multi tenancy, zoning & micro-segmentation, security visibility, secure virtualization (sVirt), trusted image signing, virtual Firewalls, DoS protection, Trusted platform module (TPM), Hypervisor & Host OS security to secure data and resources.		
9.2	The proposed solution shall support integration with Etisalat/Leading Container Security Solution, where applicable, to scan the container images and ensure malware protection of CI/CD pipeline.		

Note: "Suppliers must inform EA Cybersecurity of any non-conformity with defined EA policies and processes that are agreed upon in advance to acquire a written approval from EA Cybersecurity Department or senior management as required otherwise Supplier will be responsible for all the potential losses."