**REQUEST FOR INFORMATION (RFI)**

**IMPLEMENTATION OF SECURE DIGITAL CREDENTIALING AND QR CODES FOR ENHANCED CERTIFICATE SECURITY AND FRAUD PREVENTION**

**1. Introduction**

Umalusi is the Council for Quality Assurance in General and Further Education and Training in South Africa. Our core mandate includes the quality assurance of assessment and the certification of qualifications. The integrity and authenticity of certificates issued by Umalusi are of paramount importance. Currently, we seek to explore advanced security measures to combat the increasing sophistication of fraudulent certificates.

This Request for Information (RFI) is issued by Umalusi to gather information from interested and qualified solution providers regarding the implementation of secure digital credentialing solutions, including the use of advanced QR codes and related technologies, to enhance the security features of our certificates and prevent fraudulent activities. Umalusi is particularly interested in solutions that offer real-time verification capabilities, robust anti-counterfeiting measures, and seamless integration with existing systems.

**2. Bid Timetable**

This timetable is provided as an indicative outline of the timing of the bidding process and is subject to change at the discretion of Umalusi. Bidders must submit proposals that will facilitate the achievement of the intended commencement date.

|  |  |
| --- | --- |
| **Activity** | **Date** |
| Advertisement of bid |  28 September 2025 |
| Bid document available |  29 September 2025 |
| Briefing session |  None  |
| Closing date for bid enquiries |  10 October 2025 All enquiries must be directed to: tenders@umalusi.org.za |

|  |  |
| --- | --- |
| Closing date and time |  31 October 2025 @16H00. |
| The Email subject / Ref No. |  Umalusi (25-26) T0004 |
| Method of submission | Email |
| Submission email address | tenders@umalusi.org.za |

**3. Purpose of this RFI**

The primary purpose of this RFI is to:

* Gather comprehensive information on secure digital credentialing technologies, including Visible Digital Seals (VDS) and dynamic digital seals, and their application in securing official documents, specifically educational certificates.
* Understand the technical requirements, implementation complexities, and potential benefits of integrating such solutions into Umalusi's certificate issuance process.
* Identify potential solution providers with proven expertise in secure QR code generation, real-time verification systems, and advanced anti-fraud solutions for high-stakes documents.
* Assess the feasibility, scalability, and cost-effectiveness of different secure digital credentialing approaches.
* Inform future procurement processes, including potential Requests for Proposal (RFPs).

**4. Background**

Umalusi issues a significant number of certificates annually across various qualification. While current security features on these certificates are robust, they remain susceptible to sophisticated fraudulent attempts, including those leveraging advanced digital manipulation and AI. There is a critical need to introduce an additional layer of verifiable security that is dynamic, difficult to replicate, and easy for relevant stakeholders (e.g., employers, educational institutions, government agencies, international bodies) to authenticate in real-time or near real-time. We are seeking solutions that can combine physical document security with a strong digital verification component.

**5. Scope of Information Requested**

Umalusi is interested in solutions that address, but are not limited to, the following aspects:

**5.1. Secure Digital Seal/QR Code Technology and Security Features:**

* Describe the proposed secure digital credentialing technology (e.g., Visible Digital Seal (VDS), dynamic digital seal, secure QR code, blockchain-anchored solution). Please specify how it integrates with or replaces traditional QR code functionality.
* Explain in detail how your solution enhances the security of the certificate and specifically prevents counterfeiting, alteration, and complete fabrication, even with the use of advanced AI tools.
* Detail the cryptographic principles and other security measures embedded within or linked to the digital seal/QR code that make it tamper-proof and resistant to forging. This should include details on:
	+ Digital signatures (e.g., PKI-based, certificate authority involvement).
	+ Encryption methods.
	+ Hash functions and their role in data integrity.
	+ Protection against replay attacks or unauthorized duplication.
* How is the integrity of the digital seal/QR code ensured once physically printed on the certificate? Are there recommended printing techniques or specialized materials (e.g., security holograms, foils, inks) that integrate with your digital solution?
* What measures are in place to prevent the tampering or unauthorized alteration of the digital seal/QR code data or its linked information at any point?
* Does your solution support **offline verification** where the digital seal/QR code itself contains cryptographically signed data for initial validation without immediate internet access? If so, what data subset is typically included, and how is it secured?

**5.2. Data Encoding and Verification:**

* What type of data can be encoded within the digital seal/QR code (e.g., certificate holder's name, qualification details, issue date, unique certificate ID, digital signature, issuing body details, status)?
* Describe the process for generating unique, cryptographically secure digital seals/QR codes for each certificate, ensuring robust randomness and resistance to prediction.
* Explain the mechanism for verifying the authenticity of the certificate using the digital seal/QR code, including:
	+ Methods available for stakeholders (e.g., employers, educational institutions) to scan and verify (e.g., standard smartphone camera, dedicated mobile application, web portal).
	+ How is the *current status* of the certificate (e.g., "valid," "revoked," "suspended") verified in real-time against Umalusi's database? Describe the architecture for this real-time link.
	+ What information is displayed upon successful verification, and how is its accuracy and authenticity guaranteed?
	+ What are the failure mechanisms (e.g., "invalid," "tampered," "revoked") and how are they clearly communicated to the verifier?
* What measures are in place to prevent unauthorized access to the verification system and protect sensitive certificate holder data, adhering to principles of data minimization and least privilege?

**5.3. Integration and Implementation:**

* Describe the proposed integration process with Umalusi's existing certificate issuance system. Please specify common platforms, APIs (e.g., RESTful APIs), or data exchange formats (e.g., JSON, XML) your solution supports for automated data synchronization and seal generation.
* What are the hardware and software requirements for implementing your solution within Umalusi's environment (e.g., on-premises servers, cloud hosting, specific operating systems or databases)?
* What is the estimated timeline for implementation from proof-of-concept to full deployment, including any necessary data migration or system adjustments?
* What level of technical support and training is provided during and after implementation, including ongoing maintenance, updates, and troubleshooting?
* Describe your approach to data privacy, data residency, and compliance with relevant South African regulations, specifically the Protection of Personal Information Act (POPIA). Where is the data processed and stored?

**5.4. Anti-Fraud Capabilities and Reporting:**

* How does your solution specifically address and mitigate common certificate fraud techniques, including those involving sophisticated image editing software, AI-generated content (e.g., deepfakes), or attempts to replicate existing security features?
* Can your system detect and flag suspicious activities such as:
	+ Multiple verification attempts for a single, potentially fraudulent certificate.
	+ Verification attempts from unusual geographic locations.
	+ Patterns that might indicate a widespread fraud attempt.
* Are there any audit trails, comprehensive reporting functionalities, or automated alert mechanisms to track verification attempts, identify potential fraud patterns, or notify Umalusi of suspicious activity? Describe the type of actionable intelligence provided.
* Does your system offer a mechanism for Umalusi to instantly revoke or suspend a certificate's validity, with this status immediately reflected upon verification via the digital seal/QR code?

**5.5. Scalability, Reliability, and Support:**

* How scalable is your solution to accommodate Umalusi's current and future certificate issuance volumes, which can be substantial and fluctuate (e.g., peak matriculation periods)?
* Describe the reliability and uptime of your proposed system, including any Service Level Agreements (SLAs) you offer for performance and availability.
* What are your disaster recovery and business continuity plan to ensure continuous operation and data integrity in case of unforeseen events (e.g., power outages, cyberattacks, natural disasters)?
* Describe your support model, including hours of operation, response times, and escalation procedures.
* Describe the dependency of Umalusi on your solution once implemented and digital certificates were issued and the contract is terminated.

**5.6. Physical Document Integration (Optional but preferred):**

* Does your solution integrate with or recommend physical security features (e.g., unique security holograms like KURZ KINEGRAM/TRUSTSEAL, special inks, unique numbering, paper security features) to provide a multi-layered defence against counterfeiting?
* If so, please describe these complementary physical security elements and how they are integrated with the digital seal/QR code for enhanced protection.

**5.7. Cost Considerations:**

* Provide an estimated cost breakdown for the proposed solution, including:
	+ One-time setup/implementation costs (e.g., integration fees, software licensing for initial deployment).
	+ Per-certificate licensing or usage fees (if applicable, please provide tiers for different volumes).
	+ Annual maintenance and support fees.
	+ Costs associated with any required third-party hardware or software licenses.
	+ Any other recurring or one-time costs associated with your solution.

**6. Submission Requirements**

Interested parties are requested to submit their responses electronically totenders@umalusi.org.za by 10 October 2025. The submission should include:

* A cover letter expressing interest and providing full company contact details.
* A detailed response addressing all sections outlined in Section 4 (Scope of Information Requested) but not limited to these sections. Please clearly label each section.
* Case studies or examples of similar successful implementations, particularly in the education sector or for high-security document issuance (e.g., government IDs, professional licenses).
* References from clients where similar solutions have been successfully deployed.
* Company profile, including a description of your experience and expertise in secure digital credentialing, document security solutions, QR code technologies, anti-fraud measures, and any relevant partnerships (e.g., with security print material suppliers).
* Any relevant certifications, accreditations, or industry standards your company or solution adheres to (e.g., ISO 27001 for information security, ICAO VDS compliance).
* Service providers are encouraged to add any additional information relevant to the project.

**7. Disclaimer**

This RFI is for information and planning purposes only and does not constitute a solicitation for bids or proposals. No contract will be awarded based on this RFI. Umalusi will not reimburse respondents for any costs incurred in preparing their response. Umalusi reserves the right to use any information submitted in response to this RFI in its future procurement processes. Submission of a response does not create any obligation for Umalusi to issue a subsequent RFP or to enter into any agreement with the respondent. All information submitted will be treated as confidential.