WHITE PAPER

BEST OF TENDERS: TWO FACTOR AUTHENTICATION

Date of last revision: 2013-07-04

VERISEC

info@verisec.com
Phone (toll-free): 0800 917 8815

www.verisec.com

Introduction

The following whitepaper is intended as a guide to establish tender requirements for a strong authentication solution based on open standards. This document is primarily aimed at local government but is equally applicable to any other businesses requiring strong authentication. The open standard for authentication is called OATH, and more information can be found on http://www.openauthentication.org/ . Three compelling reasons for choosing open standards based authentication solutions before proprietary equivalents are:

- **Security**: Open Standards are documented and public and therefore well tested. Proprietary algorithms may be secure, but are often not public and have not gone through the same testing by a large critical audience.

- **Money**: Open Standards have lowered barriers to entry to the strong authentication market, thereby resulting in more vendors and lower pricing as result.

- **Freedom of choice**: By adopting open standards, products can be sourced through multiple vendors allowing for freedom of choice in terms of vendors and devices that match current and future requirements.

This guide has been created based on a collection of actual tenders that have been published in the UK during 2010-2013. The questions included in this tender cover a wide range of functionality and requirements that may be more or less applicable to the specific organisation/ IT environment. For this reason the author of this document has chosen to include a column called "Why is this relevant?" to explain when and why a specific requirement is relevant.

In addition the author has chosen to include a suggested weighting according to the following scale: M(andatory) or O(ptional).

The document is available in both PDF and Word format to allow the reader copy/paste functionality. None of the information contained in this document is proprietary to Verisec and can be copied at will.

Strong authentication can be used in a variety of solutions such as remote access, portals, single-sign-on etc. This document includes requirements that address the most common use cases of strong authentication.

The author of this document hopes that this Best of Tenders document will be useful and save time in collating requirements for strong authentication. Should there be any errors in this document or missing requirements that the reader feels would be valuable for other readers please contact Verisec on info@verisec.com with any remarks or suggestions.

The guide is structured in 3 main categories:

- **Evaluation Criteria**
- **Functional requirements**

  - General
  - Using 2FA with External Parties
  - Security
  - Logging and Monitoring
  - API Requirements
  - Scalability and Use Cases
  - User Devices and Backup Methods of Authentication
  - User Provisioning
  - Training
  - Licensing, Maintenance and Support
  - Other Requirement

- **The Damage: Commercials**

Abbreviations used in this Whitepaper:

OATH	Open Authentication Standard- see also http://www.openauthentication.org/
LDAP	Lightweight Directory Access Protocol
RADIUS	Remote Authentication Dial-In User Services
API	Application Programming Interface
EAS	Employee Authentication Scheme
OCRA	OATH Challange Response Algorithm
2FA	Two Factor Authentication
VPN	Virtual Private Network
SSL	Secure Socket Layer
TLS	Transport Layer Security
PSN	Public Sector Network

Evaluation Criteria

The questions in this section have a pass/fail weighting. Tenderers failing 1 or more of these pass/fail criteria will be eliminated and the rest of the evaluation matrix will not be considered. [In this section you might also want to include Company information which will not be scored, but should be mandatory.]

Technical Architectural Diagram

Provide a detailed architectural diagram of the proposed solution. This diagram is required as an overview for visual understanding. Failure to provide an illustrated logical overview will be deemed a fail.

[Provide space for diagram or allow for attachment]

Technical References

The award of the contract to the successful renderer will be subject to satisfactory references being obtained. Satisfactory means a positive response from each reference sought by the council. Failure to provide this information will result in your tender being awarded a fail.

	Referee 1	Referee 2
Organisation name:		
Full Postal address (including phone number):		
Contact Name (including email):		
Annual value of contract:		
Description of contract:		
Contract period:		

Delivery Timeline

The delivery timeline section will be scored on a pass/fail weighting. The council expects, following award of contract, resources to be available from the [DATE] to implement as required.

Implementation to start: DATE
Completion date (go-live): DATE
The system is expected to be fully operational by: DATE

Verification Response	

Examples of other information you may want to include in the evaluation criteria section are:

- Financial information
- Insurance details (e.g. requirements with respect to employers liability insurance, public liability and professional indemnity insurance)
- Councils Standard terms and conditions: Do you accept or not?
- Data Storage (if any data is stored off-site as defined by Data Protection Act 1998)

Functional Requirements

No.	***Requirement Description***	***Why is this relevant***	***Suggested weighting***
General			
	The authentication server must support industry standard Two Factor Authentication (2FA). Please specify how the system/application meets this requirement.	Strong authentication or two-factor authentication is a requirement for CoCo compliance. Two factor authentication refers to the use of two factors such as technical (something you have) and knowledge (something you know). An example of two factors is the ATM card with PIN. In this case the card is the technical factor and the PIN is the knowledge factor.	M
	The token authentication server must be OATH compliant	OATH is the open standard for authentication. Among the more compelling reasons for adoption is the avoidance of being locked into proprietary and possibly expensive formats and thus, possibly, limiting options in the future. For more information see OATH homepage on: http://www.openauthentication.org	M
	The authentication server must be able to connect to Microsoft Active Directory or other LDAP directory in order to validate users and store token identities.	Most organisations use a LDAP directory to manage users. By reusing an existing user repository, it is possible to avoid having management of users in multiple systems. This saves money in terms of running costs for administration. Enter the appropriate LDAP in the requirement.	M
	The authentication solution should support multiple LDAP directories.	This question is to ensure that the solution may support multiple LDAPs. For some organisations, users may reside in one or more existing LDAPs, whereby this requirement is interesting.	O

	The authentication server must be able to authenticate users from VPN (including SSL VPN) solutions using the RADIUS protocol. Specifically the solution shall support [Enter specific vendor here, e.g. Cisco, Checkpoint, Juniper...]	This requirement is valid if the authentication solution is intended for use with VPN solutions such as Cisco, Juniper etc. Most VPN solutions available on the market today support the RADIUS protocol, and by supporting this the authentication server allows for flexibility in replacing the VPN itself without affecting the authentication solution in the future.	M
	Describe how the proposed solution can run in a virtual environment. [You may want to be more specific – e.g. WM Ware]	Relevant if you are running a virtual environment and want to avoid appliance servers.	M/O
	Describe how the solution can be used for two factor authentication of internal users to web portals.	Over and above using strong authentication for VPN access it is beneficial if the infrastructure can be reused for application security, for example when authenticating users to portals or landing pages.	O
	For reason of disaster recovery, the authentication server must be able to be deployed in a dual site resilient model, with one server on each site. The servers should be able to operate in live-live mode with mirrored data for authentication.	In order to provide a high quality of service the authentication server should be able to run in parallel with another unit such that if one instance fails, transactions can be directed to the other without loss of service. In such case it is essential that the supplier explains how the reusal of consumed OTP is prevented.	M
	Specify how a resilient solution is configured and any specific requirements related to this including licensing.	Should a resilient solution be required it should not take an arm and a leg to setup. It is therefore worth checking how a resilient solution is setup and maintained over a period of time, particularly in bringing back to full capacity after a failure of one part or of the whole solution.	O
	Credentials can be issued quickly and with little effort to avoid delay to service provisioning.	General. How are the credentials issued, i.e. what effort is required to allow a user to authenticate using	M

		the system.	
	Detail a logical diagram showing the information flows between systems, and any custom middleware/interfaces that may be required. Where the solution will interact with other systems the nature of the interface and the protocols must follow industry standards and best practice e.g. LDAP, SOAP etc.	This question is to document the logical flows of information between components in the proposed solution. It is important to understand the protocols used in communication with other systems such that this does not create a problem in the future. By following open standards for communication, there is a good probability that the authentication solution can be used together with other systems, both existing as well as those that come in the future.	M
	Detail the minimum and recommended hardware and software requirements for the proposed solution. This should include server, end point devices and additional supporting peripheral requirements.	This question relates to the components necessary for a complete solution and to identify any additional costs that may arise due to the implementation of the authentication server.	M
	Detail the solutions network requirements e.g. Any Quality of Service, latency, minimum and recommended bandwidth, real time etc. This must state the minimum and recommended specifications. Benchmark results showing the system access times and performance should be provided along with a technical specification of the test network used	This question relates to the network requirements that are necessary for a working solution and to identify any additional costs related to the solution.	M
	The solution should be scalable. Tenderers are asked to describe how their solution can be expanded to meet any future needs and detail any limitations. This includes both in terms of licensing costs and technical/physical limitations.	Strong authentication can be extended to larger user groups over time. This questions help clarify whether the solution has any restrictions both in technical terms and what the cost implications would be.	M
	Please provide details of the migration path from the council’s existing	This requirement is only relevant if you are currently using a 2FA	M

	infrastructure. At a minimum the migration path should include little/no disruption to live services.	solution that you wish to migrate away from.	
	The supplier must provide a detailed infrastructure design with a corresponding project plan implementation documentation. This must include a breakdown of the activities, timescales, milestones, resources and efforts included to meet the LA/Councils timescales [specify].	General information	
	A test environment should be provided in the proposed solution that mirrors the production environment.	If you have a test environment for enabling testing of patches before live production you may want this included in the proposed solution to understand the commercial impact.	M
Using 2FA with External Parties			
	Detail how the validation software may interface with the Government EAS and/or the LPSN (London) solution to enable the use of centrally issued tokens within the council/ Local Authority.	This requirement is valid if the council/LA is looking at adopting the Employee Authentication Scheme or the LPSN in the future and may want to reuse the tokens issued by government services for local access. The employee authentication scheme (EAS) is operational but to date does not support the option of managing local authentication. This functionality has been announced previously, but no date has been set.	O
	The council/ Local authority may use the authentication solution to enable partners such as consultants, NHS or Police to gain access to the network. Detail if there are any constraints in licensing around this arrangement.	Typically, other user groups such as external consultants or partners such as the Police may need to be granted access to the LA/Council network. This question relates to any licensing issues that may arise when adding these user groups to the authentication service and to avoid unwelcome surprises.	O
	The LA/council may in the future work with other local authorities in shared services initiatives (PSN). Describe	In a number of areas local authorities or councils are cooperating around public service	O

	how the proposed solution can be deployed in this environment, if the LA/council could offer strong authentication as a service to other councils, and what the licensing implications would be related to the deployment options. The vendor should also specify any previous experience or customer references that have deployed the technical solution in this configuration.	networks (PSN). In some cases one council may wish to host authentication on behalf of other councils. This question relates to using the authentication server in a PSN environment, deployment options and the licensing implications around this.	
Security			
	All keys stored within system / application databases are fully encrypted using an industry standard encryption such as 3DES or better, ensuring keys are contained and maintained in a secure environment. Describe how keys are protected.	Each token device is loaded with a unique key that is shared with the central authentication server. This question relates to how this key information is protected in the server environment to avoid leakage of key data. In some cases the usage of a hardware security module might be required to protect keys in the system, if so, the solution should support their usage.	M
	Does the product support hardware cryptography?	Security threats are on the increase and whilst not needed in the short run it is likely that authentication servers will be required to protect token secrets with hardware encryption in the future (speculation by the author).	O
	The authentication solution should comply with the requirements of PCI DSS	If relevant, this requirement should be included. PCI DSS requirements are typically associated with systems related to payments. If no such system is to be protected using the solution this may not be a relevant requirement.	O
	The authentication solution should comply with the requirements of GSX Code of Connection	If relevant, this requirement should be included. The CoCo requirement relate to the to the Government Extranet and the level of security required by local government to	O

		access.	
	Data security and encryption is appropriate to the type and classification of data in both storage and transmission. [If you have specific requirements related to the classification of data this can be entered here]	Different methods of communication and levels of information classification may require appropriate security measures to be taken. If relevant, this question needs to be revised by the individual organisation.	O
	Describe how authentication traffic is protected?	This questions related to the protection of the authentication transaction such that information related to the transaction are not revealed in clear. This would defeat the entire purpose of the solution.	M
	All passwords and/or sensitive information stored within system / application databases are fully encrypted using an industry standard encryption level such as 3DES or better, ensuring passwords and/or sensitive information are contained and maintained in a secure environment.	This question helps understand what protection mechanisms are used for data at rest used by the system in aid of any information security audits that the organisation may be subjected to.	M
	Detail back-up and restore requirements/procedures.	All servers can fail due to hardware/ software malfunction. This question relates to how an instance of a server or appliance quickly can be put back into service by restoring earlier configurations.	M
	System access is blocked and user account suspended (lockout) after a configurable number of failed user login attempts.	If a user attempts to log-on using faulty credentials, it should be possible to lock the account after a configurable number of attempts. If a device is stolen, and used for an attempted hack, the account should be locked such that no further attempts can be made.	M
	Detail options available in the proposed solution to configure authentication options for various applications or user groups?	Checks the flexibility to tailor authentication for varying applications or users within the organisation. For example, the requirements for teachers accessing a web-based education portal might	M

		be different to employees accessing the network remotely which are, in turn, different to administrators configuring network equipment. Solutions that provide this functionality will provide better value for money in the long run.	
Logging and Monitoring			
	Systems / applications maintain complete system activity and transaction logs in support of non-repudiation and application governance.	The authentication system should be able to provide logging information related to authentication decisions, both for troubleshooting as well as for non-repudiation purposes. The solution should provide options to easily integrate with practices within your environment. Examples include central logging, own logs, ability to generate alerts and similar.	M
	The system provides real-time log viewing	Primarily for troubleshooting during setup, but also for monitoring of suspicious activity, it is valuable if the system provides a real-time log viewer as a native part of the product.	M
	Describe reporting facilities built into the product, for example, information about the tokens, or token usage	In order to support the token lifecycle the solution should be able to generate reports on token usage, allocation and similar.	M
API Requirements			
	Detail any APIs that the validation solution supports, and how these may be used.	To maximise the value of the investment in two-factor authentication solutions you may want to integrate the authentication solution with legacy systems, single-sign-on solutions or equivalent. In these instances you may need access to an API that allows for programmatic authentication requests.	M

	Tenderers must define any additional cost that may arise from the access and use of these APIs.	Just to make sure if there are any hidden costs.	M
	The authentication solution should provide support for WS-Trust and SAML2	SAML2 is an open standard for passing authentication information to other systems, including a number of cloud based systems. By supporting the issuance of SAML2 assertions, authentication information can be passed on internally to other systems, or to external partners. Likewise, WS-Trust provides a standard authentication interface allowing application connectivity with little or no integration efforts.	M
	SAML2 assertions shall be digitally signed under a configurable PKI	Digital signatures assure authenticity and integrity of SAML2 assertion to consuming applications. It is essential that it be configured under what PKI the SAML2 assertions are signed.	M
	Tenderers should identify any mechanisms in place to request enhancement of API functionality	This helps you identify what extension mechanisms the vendor provides should you have custom authentication needs. You may also want to change the wording of this question to relate to any professional services that the vendor can provide to write specific functions using the API calls.	O
Scalability and Use Cases			
	A solution that is scalable initially up to X users and has the capability to be expanded beyond. [X being the number of intended users of the system. You may want to include groups of users that today are not included in order to make sure the solution can scale]	It is important to know not only whether the authentication solution supports your current number of users, X, but also how this might scale up in terms of additional users in the future. Bear in mind that additional user groups might come from other applications – for example, if you are looking for an authentication solution for VPN access, the user growth in that area	M

		might not be huge, but you could provide better authentication to a school portal in the future and therefore add a significantly larger number of users.	

User Devices and Backup Methods of Authentication

	The OTP (One Time Password) tokens can be event or time based	Standard functional requirement	M
	The OTP tokens are OATH compliant.	Requirement to support the Open Authentication Standard	M
	The design battery life of the token device must be greater than 6 years. Detail the assumption underlying the design figure, such as number of OTP generated per day.	Unless the battery can be changed which is unusual in new tokens, the expected lifetime should be as long as possible.	M
	Tokens should be 1m water resistant in compliance with the IPx7 standard	Most people don’t swim with the token daily, but accidents involving soft drinks should not affect the device.	M
	Tokens should be available in a keyring form factor with one button. Pressing the button gives an OTP. Please describe the available options.	This requirement relates to the form factor of the token device. Can be removed if you wish only to have another type of device.	O or M
	Tokens should be available with a PIN pad that requires the user to enter a personal PIN on the pinpad before accessing the OTP	This requirement relates to the form factor of the token device. Can be removed if you wish only to have another type of device.	O or M
	Detail any backup authentication mechanisms available if a physical token device is lost or misplaced. Specify any interfaces that may need to be configured as well as any additional costs for licensing or implementation.	Regardless of the token bearer (physical token or mobile phone) user can and will displace them at the most inconvenient of times – this requirement helps you identify what mechanism, if any, the authentication solution provides to alleviate the inconvenience in such situations. In other words, where the internal security policy allows for this a temporary or backup solution should be available to the	M

		user until such a time where a new authentication device can be issued or the original is located.	
	Token should be available with a combined RFID & OTP “Display Card” for a unified staff identity and building access solution. Detail available options.	This requirement related to the ability of combining the OTP technology with RFID technology such that users can enter the building using the same card. Can be removed if you wish only to have another type of device.	O
	Support for mobile devices. Please specify operating system (Windows Mobile, Android, iOS and Blackberry)	If you want to use mobile phones as token bearers this question helps you identify whether the solution will cover the platforms that your end-users have.	M/O
	A solution that support multi form factor tokens (hardware and software tokens) so that We have the flexibility to provide tokens which are a best fit for requirements	Not all end-user groups have the same requirements and it is worth knowing what flexibility you have in coping with the variation.	M
	Detail the physical characteristics of the proposed token including vibration/drop resistance along with reference to the relevant IEC/ISO/EN standards used.	Just to get a better picture of the physical token.	M
	The LA/Council has existing assets which may be used in the new solution to reduce costs. The supplier should detail how existing assets can be reused as part of the proposal. [Requires information regarding the existing solution to be provided as part of the tender]	Only relevant if you are migrating from an existing solution.	

	Describe any options that are available to support visually impaired users that cannot read a conventional “display” token	The Disability Act requires you to provide an equal level of service to users with disabilities. This helps you identify the supported options.	M
	Describe the token lifecycle during a typical deployment, including issuance, revocation, replacement, and de-provisioning.	A good solution will have minimal impact or will even simplify your existing user-management processes for joiners, leavers and movers within the organisation.	M
	Detail any options related to tokens such as branding with logos, colours etc.	Most vendors will have options for branding the tokens. Depending on the volume there may be additional costs.	O
User Provisioning			
	The vendor should specify if they can manage distribution of tokens to the end users. [Depending on the organisation you may want individual tokens to be distributed or in batch.]	An important aspect of the roll-out will relate to the distribution of the physical device. If the devices will be handed out centrally this will not be a relevant question	O
	How are the tokens programmed and the key files distributed? Please specify physical and logical security procedures.	A core security concern in authentication solutions is the unique key stored in each device. The vendor should be able to show how this information is entered into the token, and secured in transport. At no time should the key files be exposed in an open network environment.	M
	Can the vendor provide PIN envelopes for initial activation PIN or unlock codes?	In some cases you may want to distribute tokens with a PIN pad with a unique initial PIN that is changed on first use. The vendor should be able to provide the PIN envelopes such that these codes can be securely distributed. An alternative might be sending out the initial PIN using SMS, which will require prior knowledge of the mobile telephone numbers.	O

	Describe any services that you provide related to warranty returns and environmental destruction.	Although token technology is quite robust today it is nevertheless worth knowing how warranty claims are handled and what options the supplier provides in terms of disposing safely of tokens that are no longer in function.	
	The system shall provide a centralised management interface. Describe.	General information.	
Training			
	The winning tender will be required to provide training on the OTP token product set. This training programme must cover: • Authentication server management: full configuration and support. • Token lifecycle management. • Integration with user directory. • Backup and Restore Procedures Training should be for a minimum of two administrators and three support engineers and be included in the overall contract cost.	Providing a good level of service requires trained staff, both from an administrative perspective as well as from an operational/helpdesk perspective.	M
	Provide full details of the training provided.	General information	M
	The supplier should indicate whether the training is on-site or off-site.	General information	
Licensing, Maintenance and Support			
	Detail the licensing model for the proposed solution.	All vendors are not created equal.	M
	The licensing model for the validation servers must be detailed for the initial X users, and how this can be expanded for future requirements.[Specify the number of initial users]	The same question as the one in the technical section except that here the vendor should describe licensing implications for current and future user populations.	M

	If the authentication platform is used with other authorities- what is the licensing effect?	In case you decide to have a shared authentication service with, for example, neighbouring local authorities, what are the licensing implications of this?	O
	If the solution is used with external parties such as consultants- will there be a licensing effect?	Looking for any hidden costs	O
	Is there any licensing effect if the solution is used with multiple applications such as VPN, Web portal access etc.	Looking for any hidden costs	O
	Any limitations in the number of users support must be supplied	Important if the solution is intended for a larger audience or for use in a PSN environment.	M
	All Tenderers must provide product support and a route to escalate technical issues directly to the product vendor**.**	Describe the support organisation	M
	Describe the fault escalation process available to the customer.	Describe the support organisation	M
	Provide an overview of your support and maintenance service including: Levels of service e.g. 24/365, business hours, etc. • Type of support (email, telephone, on-site) • Response time • Resolution time Please detail support packages offered.	Describe the support organisation	O
	Suppliers must indicate if there is a published release cycle indicating how many software and/or patch releases have been issued in the past 12 months.	General information- you may not want too many updates.	
	Tenderers are requested to provide information and resource to assist IT Services in completing an Operation Support Guide.	Exploring willingness to assist with material that should be readily available at a vendor.	O

	Please state your willingness to assist with this exercise.		
	Detail how you can ensure the Council will remain on a current and supportable version of the solution. Including all supporting components and add-ons e.g. Java, Flash, Shockwave etc.	Helps identify what is the effort required to upgrade when new version of the authentication solution are delivered to the council. Generally, the less dependencies, the better.	M
	Detail how often on average new releases and versions are made available and how an upgrade procedure is performed. Also specify if there are any costs related to new patches, releases or version upgrades.	New versions and releases are typically made available over time and may require extensive administrative overhead to implement. The question relates to the cost of maintaining the system over time. In addition, some upgrades may require a license fee to be paid.	M
Other Requirements			
	The tender shall be able to provide the Council with X tokens within Y weeks of legal acceptance of this tender.	Makes sure that the supplier can deliver to your project requirements.	O

The Damage: Commercials

	Tenderers must state clearly the full costs for all goods and services to be supplied as part of this proposal. [You may want to be more specific and detail number of licenses needed, tokens, test environment, hardware & software]	Good understanding of the costs.	M
	Contract maintenance charge for 3 years (should include all parts of the proposed solution).	Part of the running costs of the solution. Or for whatever period you are looking at for the investment	
	Please describe your preferred method, including review periods, for identifying and charging for licences added or removed during the term of the contract.	How will this work in practice?	M
	Branding Please supply costs for branding the device with a Council logo and text.	You may want your own logo	O
	Please specify costs for Installation of the proposed solution including time estimates.	Good understanding of the costs	M
	Please specify costs for Training of the proposed solution including time estimates and any limitation on the number of attendees.	Good understanding of the costs	M