

Security & Support Services

Access Control Specification Document

1. General System			
1.1			
1)	M		The access card should carry the user's identity while the system should validate the rights for that identity
2)	M		To be NFC compatible
3)	M		On-line locks can use Power over Ethernet (PoE) either directly or indirectly
4)	M		Locks should be tested to a minimum of minus 15 degrees centigrade in dry and wet conditions
5)	M		Off-line locks to be capable of receiving a direct power supply in lieu of batteries to facilitate emergency access
6)	H		The encryption technology used must be robust and resistant to unauthorised manipulation and cloning
7)	H		The system must be capable of speedily updating off-line locks
8)	H		Off-line locks must be capable of speedily updating the control database regarding matters such as audit trail, battery condition and fault detection
9)	H		On-line locks must use standard TCP/IP protocols and operate over multiple sub-nets and address ranges
10)	H		All lock cabling must be over structured wiring to category 5E or better

11)	H		The system must use a contactless technology, such as RFID to ISO 14443 or equivalent, with an option to expand later to newer technologies. (Tenderers must specify and detail their technology and protocols used)	
12)	H		Access control cards must be capable of holding other information as the client required, electronic and pictorial.	
13)	H		Suppliers must state the technology and spare data capacity of the card	
14)	H		Suppliers must specify how many on-line locks are managed by their local controller	
15)	H		Battery power supply to off-line locks must be located on the interior side	
16)	M		Suppliers must specify how off-line locks report battery failure	
17)	H		Suppliers must specify the average battery life and its associated number of transactions	
18)	H		Suppliers must specify the type of battery required for differing weather conditions	
19)	M		The locks must be capable of being used by multiple users. Each user must be able to gain access to multiple locks and these access rights must be able to be granted both individually and as user group(s)	
20)	M		Suppliers must specify the minimum and maximum capability of their system in order to facilitate in excess of 40k users and 300 buildings	
21)	H		The supplier must specify the maximum number of locks their system can support	
22)	M		Tenderers are to specify the level of security provided by each of their locking systems eg: <ul style="list-style-type: none"> - BS standard - Strength to LPC standards - Recommended configuration 	
23)	M		The system must be capable of supporting both on-line and off-line locking systems from the same central database	
24)	M		The supplier must specify how their system is capable of controlling student residences/ hospitality use as well as business/academic use	

25)	M		The supplier must specify their door systems are capable of meeting all statutory requirements including: <ul style="list-style-type: none"> - fire egress - DDA 	
26)	M		The system must be supported by a single central database and managed by a number of individual areas/departmental work stations. Suppliers are to detail the number of workstations that can be supported	
27)	H		The supplier is to describe whether one or more locks can be 'locked' or 'totally blocked' from a central location, irrespective of their pre-programmed situation, thereby overriding previous contingencies in an emergency.	
28)	M		The supplier is to specify how information, ie date, time etc is passed from software to offline locking systems.	
29)	M		Supplier must have a track record of providing a rapid and high quality responses to customer support requests: <ul style="list-style-type: none"> - parts - servicing - software support - training Suppliers are to specify a minimum of three Higher Education establishments for references	
30)	M		All parts of the system must be supported for a minimum of 10 years from the date of commissioning of the each installed system	
31)	M		Suppliers to detail all additional costs, ie commissioning and training	

2. Technical				
2.1 Software System				
32)	M	Application architecture	Suppliers are to describe the software architecture, identifying key components and their inter-relationship, indicate which components are core and which are optional and what programming language(s) the system is developed in?	

33)	M	Supported platforms	<p>The system must run under one of the following operating systems:</p> <ul style="list-style-type: none"> a) Solaris 10 or later (SPARC or x86) b) Windows Server 2003R2 or later c) RedHat or Debian Linux <p>Suppliers are to provide a list of the platforms and operating environments that are supported by the system, giving full release details (e.g. Solaris 10 11/06, and indicate any significant differentiation in functionality of the system across supported platforms/environments.</p>	
34)	H	Virtualisation support	<p>The system should be supported when running on virtualised hardware, such as VMWare or Solaris Zones.</p> <p>Suppliers are to give details of your support for machine virtualization and indicate any differences in support between virtualized and non-virtualized hardware.</p>	
35)	M	Content storage	<p>Suppliers are to describe how the system stores content, eg. in a file system, in an object database, a relational database or some hybrid</p>	
36)	H	Supported databases	<p>The system should support one or more of the following for core database functionality (if required):</p> <ul style="list-style-type: none"> a) Oracle 10g or later (preferred) b) SQL Server 2000 or later c) MySQL 5 or later <p>The supplier must provide a list of the databases that are supported by the system, giving full release details (e.g. Oracle 10g R2).</p>	
37)	M	NAS filestore support	<p>Any filestore-based content would be stored using a NAS infrastructure (using Network Appliance filer systems). The system must support this technology.</p>	

38)	M	Availability during upgrades	<p>Routine systems maintenance operations, including upgrades, must be able to be carried out without disrupting the service to users.</p> <p>The supplier must describe how system availability is maintained during scheduled maintenance e.g. application of patches and installation of upgrades.</p>	
39)	M	System monitoring	<p>The system must provide facilities to monitor its overall health and thereby predict or detect failures.</p> <p>The supplier must describe the system monitoring capabilities.</p>	
40)	M	High performance/availability	<p>The supplier must describe any other high performance/availability features of the system, such as clustering, load-balancing, or any other features.</p>	
41)	H	Scalability	<p>The system must be incrementally scalable to meet changing load.</p>	
42)	M	Configurations	<p>The supplier is to provide details of the recommended hardware and software configurations for the following profiles:</p> <p>250 sub-sites 50 simultaneous active administrators high availability</p> <p>and indicate the expected response times to typical administrative activities</p>	
43)	M	Backup and recovery	<p>The supplier must state the recommended approach to backup and recovery, including the impact on performance and application availability.</p>	
44)	H	Authentication	<p>The system should be able to authenticate administrative users against the University's Sun iPlanet LDAP service, or Active Directory.</p> <p>The supplier is to describe how the system authenticates users.</p>	
45)	M	Password security	<p>Copies of user passwords must not be stored on the persistence layer of the system.</p>	

46)	M	Browser support	<p>If the system has built-in web pages (including interfaces for administration) these must be browser-independent and must be fully usable in at least the following browsers, with no loss of functionality:</p> <p>Internet Explorer 6.0 or greater Firefox 2.0 or greater Safari 3.0 or greater</p> <p>Where suitable browser releases are available, it must be possible to use these on at least Windows 2000/XP, UNIX/Linux and Mac OS X.</p> <p>The supplier is to</p> <ul style="list-style-type: none"> - State your browser support policy. - Give details of your current browser/platform support matrix. This must include version information. - Highlight any differences in functionality across the platform combinations in respect of administration, and general viewing. - List any dependencies on plugins, helper applications, etc. 	
47)	M	Multiple workstations	The system must be able to serve multiple administration workstations. The supplier is to specify the maximum number of workstations their system can support.	
2.1.1 Integration and Customisation				
48)	M	User identity	The system must work with User IDs in the form normally adopted by the University (which consist of an alpha-numeric string starting with one to five letters, followed by one to four decimal digits).	

49)	M	External role data	<p>The system must be able to read and use role data from the University's corporate systems in the assignment of privileges to users. (This role data encapsulates information such as who is a student, who is staff in a particular department. The information is stored in a variety of relational databases and LDAP directories).</p> <p>The supplier is to state how their system would integrate with such sources, including how it would keep track of external changes to source data.</p>	
50)	M	Data from external datasources	<p>The system must provide facilities to integrate data from external sources, e.g. relational databases, into system-managed content.</p> <p>The supplier is to state describe any built-in capabilities (e.g. scripting languages) to facilitate this.</p>	
51)	M	SMTP integration	<p>E-mail integration with the University's central SMTP service is required for workflow notifications etc.</p> <p>The supplier is to describe the system's e-mail functionality covering the above point and list any reliance on specific mail technologies external to the system.</p>	
52)	M	Anti-virus integration	<p>The system must integrate with or incorporate antivirus software to protect against viruses.</p> <p>The supplier is to describe how the system meets this requirement and how updates to the virus database are handled.</p>	
53)	M	Application Programming Interface (API)	<p>The system must provide fully documented and fully supported APIs to allow integration with external systems for the purposes of managing user IDs, roles and rights, and statistics within the system, with the ability import, edit, disable, and expunge IDs and rights.</p> <p>The supplier is to provide details of the supported API(s), indicating in each case whether the access is read-only and describe the security context for the use of the APIs.</p>	

54)	M	Migration (import facilities)	The system must provide tools for bulk import of user IDs from existing services into the access control system. The supplier is to describe the import tools available to support this.	
2.1.2 Licensing				
55)	M	Licensing model	The supplier is to describe the licensing model for the system and the way this is implemented.	
56)	M	Third-party licenses	The supplier must itemise any third party licenses that would be required for the system in the University of York environment. (Only those licenses directly related to the base-level operating system may be excluded from this list).	
57)	M	Separate testing/training/development systems	The licensing model must support the use of separate test, training, or development systems for trying out new materials and software releases. The supplier is to describe how this is supported.	
58)	M	Failover hardware	The supplier is to identify any licensing implications should it be desired to run the software on alternate hardware in the event of a server failure.	
2.1.3 Product development				
59)	M	Overall product development	The supplier must describe the product development path for the system, identifying the primary development platform(s) and describing the procedure for porting to other supported platforms; delays to the release for platform ports must be detailed	

60)	M	Maintenance and enhancement	<p>The supplier must meet the following requirements:</p> <ul style="list-style-type: none"> a) Regular product maintenance, development and enhancement. b) Provision of comprehensive advance information and training on new and changed features appearing in upgrades. c) Enhanced supplier support during and after upgrades. d) Automatic notification of patches and fixes. e) Advance product lifecycle warning notices, e.g. withdrawal of support for a particular database version. <p>The supplier must detail any differentiation in support levels for the different platforms, e.g. Windows vs. Unix.</p>	
61)	M	System and application housekeeping	<p>Detail the facilities provided for routine system administrative housekeeping, including</p> <ul style="list-style-type: none"> a) The roles involved b) When the tasks must be performed c) The degree of automation available <p>Identify any activities by administrators that would require direct access to any underlying database and or operating system.</p>	

3.1 Deployment				
62)	M	Staff competencies	The supplier is to describe the skill set required for each key management role within the system, e.g. administrators, reception staff.	

63)	M	Implementation support	<p>Suppliers must demonstrate that they have a well developed and tested implementation support programme:</p> <p>a) Preferably with experience of implementing their system within the higher education or public sector;</p> <p>b) With support facilities provided for the period before, during and following installation.</p> <p>The supplier must describe the implementation process and give details of typical implementation support and timescales.</p>	
64)	M	Training	<p>The supplier must be able to provide comprehensive initial training for all key role-holders within the system e.g. system manger, administrators, reception staff, maintenance etc.</p> <p>The supplier must describe the training recommended giving indicative costs</p>	
65)	M	Documentation	<p>The supplier is to provide comprehensive documentation for all relevant aspects of the system and for all key role-holders within the system e.g. system manger, administrators, reception staff, maintenance etc.</p> <p>The supplier is to list the documentation delivered with the system.</p>	
66)	H	Documentation re-use	The supplier must permit the University to re-use the vendor's documentation in locally developed materials at no extra cost.	
67)	M	Online help facilities	The system must provide online help facilities.	
68)	H	Context-sensitive help	The online help facilities should be context-sensitive.	
69)	H	Customisable help	The online help content should be customisable.	
70)	M	Product support	<p>Comprehensive software support must be available via telephone, email and the web as discussed in the Service Level Agreement (SLA). Suppliers should provide a sample SLA with their response.</p>	
71)	M	Support during working hours	Help desk support must be available during normal UK working hours.	

72)	H	Online fault-logging system	The supplier should provide an online system for problem/fault/query logging and tracking.	
73)	M	Support model	The supplier is to detail their support provision.	
74)	M	Client systems / workstations	Client systems for use by administrators must run on a standard Ethernet-networked PC platform using TCP/IP protocols. The supplier must state the required hardware configuration and Operating System requirements for such workstations.	
75)	M	Workstation connectivity	The supplier is to state any special interface requirements for the workstations, eg RS232 serial port to connect to portable programmer, interface required to connect to card reader/writer. If a serial port is required, the supplier is to state whether a USB port combined with a USB-to-serial adaptor is supported.	

4.1 Access Tokens and Security				
76)	M	Access tokens	The system must use contactless tokens to identify and authenticate users at controlled points of access. The supplier is to describe the tokens used by the system, eg are these RFID cards, smartcards, active RF devices, etc	
77)	H	Alternative technologies	The system should be capable of upgrade to accommodate developing technologies, such as Near-Field Communications. The supplier should describe any planned development to accommodate other contactless technologies.	
78)	M	Access rights storage on the token	The tokens must hold the user ID and, if applicable, membership of groups.	
79)	M	Alternative digital data	The tokens must be capable of carrying other data in the form of a standard magnetic stripe, to facilitate its use with older access control system in use at the University.	

80)	M	Other digital uses of tokens	<p>The tokens must be capable of storing additional digital information, such as library codes, car parking rights, virtual cash, and/or biometric data.</p> <p>The supplier is to describe the amount, type, and organisation of available free memory.</p>	
81)	M	Visual data	<p>The token must be capable of being overprinted with both standard and customised visual content, such as University logo, user photograph, and a barcode.</p> <p>The supplier is to describe if the token is not in the form of a card, any provision available to carry visual data.</p>	
82)	M	Access rights validation by online locks	<p>Online locks must validate the User ID and/or group membership against the central database, taking account of any permitted/disallowed times, and must not rely on access rights stored on the token.</p>	
83)	M	Access rights validation by offline locks	<p>Offline locks must validate the User ID and/or group membership against information in the memory of the lock, taking account of any permitted/disallowed times, and not rely on access rights stored on the token.</p>	
84)	M	Data security on tokens	<p>Data carried on tokens and transmitted between tokens and locks must be secure against unauthorised alteration, preferably using a published encryption scheme.</p> <p>The supplier is to describe the encryption scheme and associated security measures employed (eg Mifare, Legic, etc).</p>	
85)	M	Token security	<p>Tokens must be secure against "cloning".</p> <p>The supplier is to describe measures adopted in the system to prevent or mitigate against cloning of tokens.</p>	

5.1 Networking and Communications

86)	M	Network protocols	Online locks (or their controllers), workstations, and central servers must communicate over an Ethernet network using standard TCP/IP protocols.	
87)	M	Subnets and routing	The University of York network is a fully-routed network divided into several subnets, not all of the same size. Networked devices must support variable-length subnet masks and be able to use a default gateway to communicate with other networked components of the system.	
88)	M	Firewall traversal	The University of York uses a firewall to separate facilities networks (such as will be used for online locks and controllers) from workstations and servers. The supplier is to state how what provisions would be required to allow networked components of the system to communicate across the firewall, such as permitting particular protocols or TCP/UDP port numbers.	
89)	M	Device registration and DHCP	The University of York normally requires that network devices be registered in a LAN database, which is used for several purposes including IP address allocation. The supplier is to state whether online locks (or their controllers) can use DHCP to obtain IP information, or must be manually assigned address, gateway, subnet mask, and other information.	
90)	M	Power for lock controllers	Where network-connected controllers are used to control online locks, readers, or ancillary equipment, they should be capable of being powered using IEEE 802.3af Power Over Ethernet (PoE), drawing no more than 13 watts. The supplier is to state if PoE cannot be used directly to power controllers, the voltage and current requirements, and whether the power could be derived from a PoE "splitter".	
91)	M	Cabling to online device controllers	All networked devices such as controllers for locks and readers must connect to a standard network outlet by means of a standard Category 5e patch cord fitted with RJ45 connectors.	

92)	M	Connections from online locks to controllers	The supplier is to state how an online lock, such as one fitted in a door, is connected to the network, or to its network controller if a local controller is used. If connection is by radio, state the frequency band and range and any means employed to mitigate against interference or jamming. If connection is by wire, state the type and size of cable and how it is terminated.	
93)	M	Connections from controllers to readers and ancillary devices	The supplier is to state how a networked controller is connected to devices such as readers or ancillary devices. If connection is by radio, state the frequency band and range and any means employed to mitigate against interference or jamming. If connection is by wire, state the type and size of cable and how it is terminated.	
94)	M	Data transfer to offline locks	It must be possible to update offline locks with data, such as permitted or barred user IDs, by using a portable programming device. The supplier is to state the type of this device, and whether it is a system-specific proprietary item, or a generic device such as a handheld computer and how it communicates with the lock, ie whether by cable, infra-red, or some other means.	
95)	M	Virtual networking of offline locks	It should be possible to send data such as user IDs and access rights, and retrieve data such as an audit trail, from offline locks without requiring a portable programming device. The supplier is to state how it is achieved, eg by transferring data to and from an ordinary access token carried by a user between an offline and an online locks and state how long it takes to transfer this data from lock to token (and vice versa).	
96)	M	Data transferred to/from offline locks	The supplier is to state what data, and how much, can be carried to offline locks by each of the methods available within the system (portable programmer, virtual network, etc) and state what data, and how much, can be returned from offline locks by each of the methods available within the system.	

6.1 Features of Product

97)	M	Time Zones	<p>Must provide multiple time zones</p> <p>The supplier is to state how many time zones the system can accommodate</p>	
98)	M	Day Light Saving (GMT/BST)	<p>The supplier is to state how the product copes with changes to 'day light' saving times and how this is communicated to locks.</p>	
99)	M	Holiday Settings	<p>The supplier is to state whether individual locks can have their own individually associated calendar for holiday settings, as opposed to having only one global holiday setting. (This should allow individual departments to determine whether they are open or closed during each separate holiday period). Ideally, this should be achieved with minimal administrator input.</p> <p>The supplier is to describe how the product will cater for this need.</p>	
100)	M	Automatic Changes	<p>The system must provide the ability to program locks with automatic changes, eg open at 09.00 and lock at 17.00.</p> <p>The supplier is to state the maximum number of automatic changes allowed by the product.</p>	
101)	M	Batch Editing of Users	<p>The product must provide for the batch editing of users.</p> <p>The supplier is to describe how this is achieved</p>	
102)	M	Batch Editing of Locks	<p>The product must provide for the batch editing of doors.</p> <p>The supplier is to describe how this is achieved</p>	
103)	H	Automatic Changes Report	<p>The supplier is to identify whether their system can provide an independent report that shows/list all doors programmed with automatic opening.</p>	

104)	M	Residential Door Locks	<p>It is essential that locks used to allow entry into study bedrooms allow for the following features</p> <ul style="list-style-type: none"> • Allow entry on first swipe (or similar method) and remain open until the resident secures the lock via a privacy thumb turn (or similar device) from inside the study bedroom upon retiring or externally via a swipe (or similar method) upon leaving the study bedroom. • The privacy thumb turn cannot be overridden by service personnel, such as cleaners but allows full access rights when not in privacy mode. • Privacy can be overridden by Security in an emergency. • Egress from the residential room is by a single action of the handle <p>The supplier is to describe how the product would meet this requirement.</p>	
105)	M	Lock Programmable Remotely	Ability to programme and update lock from remote PC. The supplier is to describe how this is achieved.	
106)	M	Office Mode	Individual locks can be locally programmed to remain open when there is a need to keep the door open unlocked for a specified time period by the local user. The supplier is to describe how this can be achieved.	
107)	M	Opening of Locks with Flat Batteries	The supplier is to describe how locks with flat batteries can be opened.	
108)	M	Audit Trail	The product must provide audit trail reports. The supplier is to specify the storage capability of their system	

7.1 Maintenance				
109)	M		The supplier is to make available to the University their spares catalogue and current prices.	
110)	M		The supplier is to specify their lock materials and finish	
111)	M		The supplier is to specify their lock configuration and means of emergency access to override the various levels of locking device	
112)	M		The supplier is to provide samples of all locking devices proposed	

113)	M		The supplier is to describe anti-tamper devices	
114)	M		The supplier is to detail how each locking system is capable of functioning in wet weather/humid conditions giving guarantees/warranties.	
115)	M		The supplier is to specify how many operational cycles each locking system will withstand, ie the mean time between faults (mtbf) for each device.	
116)	M		The supplier is to specify the durability of each locking system in respect of:- <ul style="list-style-type: none"> - impact resistance of the casing - the handle mechanism 	
117)	M		Where wet cell batteries are proposed, the maintenance schedule and current replacement costs are to be provided	
118)	M		The supplier is to describe the training required to maintain the system, from software through to hardware, and detail each recommended training programme giving indicative costs.	
119)	M		The locks must remain functional by an alternative emergency power supply for a guaranteed minimum of 6 hours. Tenderers are to specify their exact proposals	
120)	M		Tenderers to identify what happens in the event of a power failure (ie means of notification) or loss of connectivity to the file server	
121)	M		Tenderers are to specify what management information is available from their system	