Date
2015-04-13

Registration number
2014-017920

Request for Information (RFI) regarding offender self-service for Swedish Prison and Probation Service

Table of content

1. Background

The vision - "better out"

The vision "better out" is based on a set of values that the Swedish Prison and Probation Service (hereafter Kriminalvården) has worked out. We want our offenders to have a better chance at a lawful life after they have served their sentences with us. Their time should make a positive difference for the transition back into the community.

To carry out our mission in a good way, we need to work closely, professionally, legally, securely and reliably with the offenders. This increases the trust that offenders and the public have for Kriminalvården.

Kriminalvården’s mission is crime prevention, increased personal safety and to contribute to a safer society.

Kriminalvården

Kriminalvården is the government authority responsible for the prison and probation service. In total there are approximately 4500 offenders spread across 47 prisons in Sweden. Furthermore, there are 31 detention centers that handle about 1800 detainees. In addition, about 2 300 offenders are in probation with electronic tagging. In general each of the offenders have their own living area.

In prison the offenders are engaged in one or more of the following activities:

- Education
- Work assignments
- Substance abuse treatment or personal improvement programs
- Other structured activities

These activities all need improved IT support to the offenders. This IT support should be designed so that the clients will get more opportunity to get digital experience for example to act as a corporate citizen both in the role of employee and in contacts with the authorities. One step in this effort is the project InIT 2.0.

The InIT-project

One purpose of InIT 2.0 project is to update the existing learning platform for prisoners. This upgrade is to increase safety but also to provide features, for e.g.:

- Improved training functions
- Increased ability for self-administration
- Improved support for program activities

2. Administrative rules

This chapter describes the administrative rules of this RFI. These rules deal with how this RFI is managed and how the answer should be handled.

2.1 The purpose of this RFI

The purpose of the RFI is to collect information about the suppliers and products on the market that can be used to develop IT support to the offenders. This RFI does not obligate Kriminalvården to any procurement. Furthermore, it is important to emphasize that those who respond to this RFI are not obliged to answer all parts of the RFI.

Answers to this RFI will serve as basis for decisions regarding eventual future procurements. This means that parts of the architecture and design might be adapted based on market response.

2.2 Requirements

RFI is sent to suppliers in the IT industry. It is free for everyone to respond to this RFI. The responses to the RFI are public documents. If the supplier wishes for any part of the answer to be kept confidential, this must be communicated to Kriminalvården. Possible future procurement is conducted under current regulations for public purchasing.

2.3 The structure of the answer

It is important to note that it is not necessary to provide all requested products. Nor is it necessary to meet all requirements for the product provider. However, requirements that aren’t met should be documented.

A supplier can offer a full solution, as long as it is built from modules in accordance with this document.

Responses to this request shall consist of four parts as follows.

<u>Part 1 Supplier Presentation</u>
The first part shall be an account in the table below.

Aspect	Content
Overall description of the supplier	An outline example in terms of customer base, history, product portfolio and history.
Standard	The standards in terms of interfaces, etc. that are supported for interactions between different parts.
Number of installations	Number of installations, or the fact that it is a new product
When available	When delivery can be made of the product.
Roadmap	What future features are planned.

Figure 1 Brief account of the supplier and the supplier's product.

Part 2 Supporting infrastructure functions
Appendix 1 describes the essential features for achieving high security and operational stability. The reply shall describe how the provider supports these features in the form of integrations. Offering these functions is described in section 3.

Part 3 Product Description
Appendix 1, 2 and 3 contain demands for infrastructure services, applications and devices. In the response to this RFI the supplier will answer how the product meets the requirements of the respective table or underlying text. The supplier must also specify the conditions that must be met for the requirements to be met.

Part 4 Costs / Business Model
This part shall indicate an estimate of the price for:

- Development
- Licenses or suchlike
- Operating expense
- The cost of adapting the product in order to fulfill the requirements

Furthermore, the provider of this part may present alternative business models.

2.4 Further information

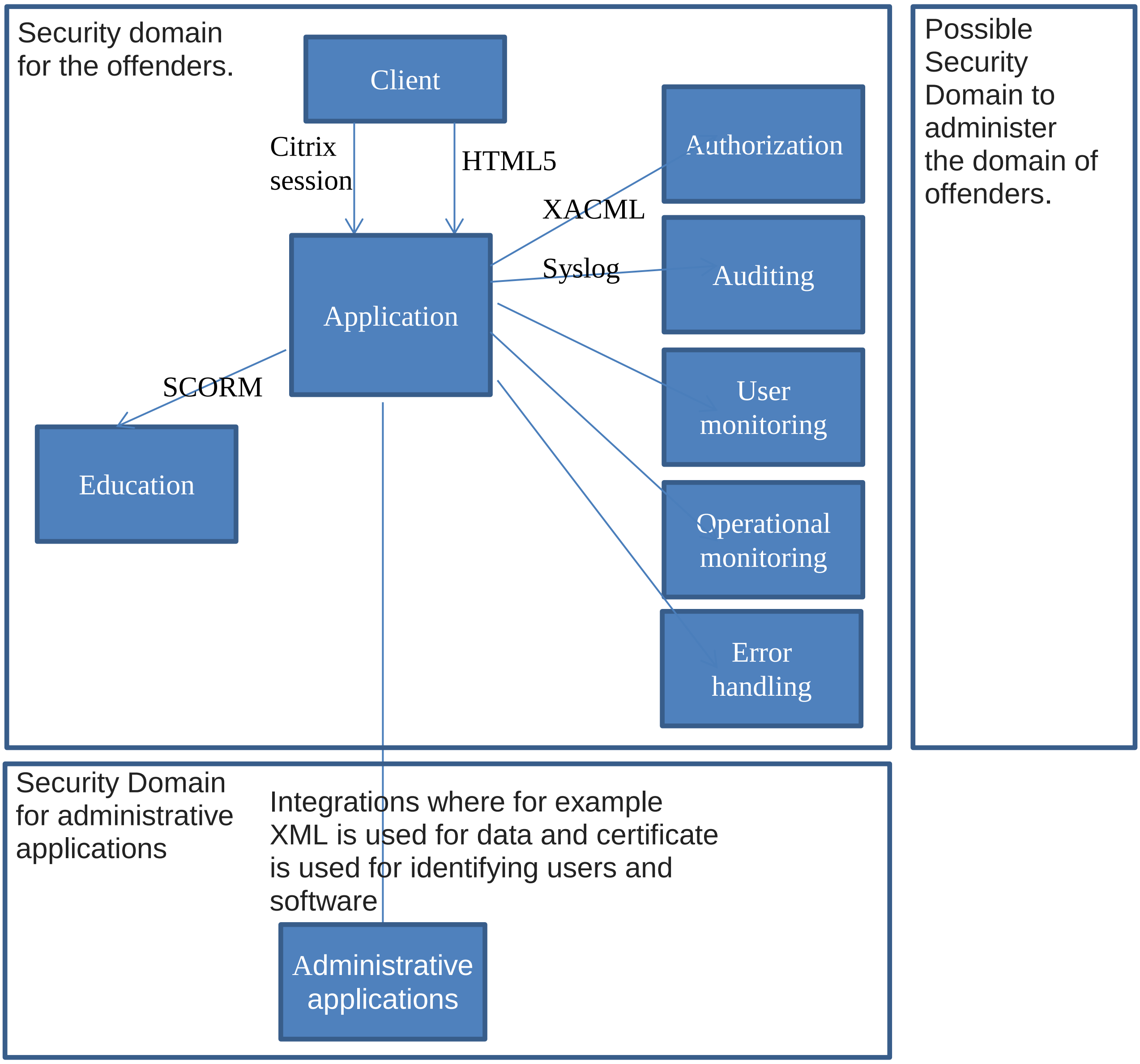
Questions regarding this RFI should be sent to:

- Leverantorsfragor.INIT@kriminalvarden.se

Answers will be emailed to all respondees, and published online at a location which will be communicated later if nothing else has been mutually agreed..

3. The idea behind infrastructure of the platform

The basic concept for the architecture of the platform is that it should be possible to choose different providers for different parts. To enable this, it is important that the applications use well-established and accepted interface. Current interfaces are specified for each application. Below is a vastly simplified picture of candidates for the interface.


Security domain for the offenders.
Client
Citrix session
HTML5
Authorization
XACML
Syslog
Auditing
Application
SCORM
User monitoring
Education
Operational monitoring
Error handling
Possible Security Domain to administer the domain of offenders.
Security Domain for administrative applications
Integrations where for example XML is used for data and certificate is used for identifying users and software
Administrative applications

The conclusion to be drawn from the above figure is that the applications should support the fixed interface to common infrastructure services. This will give Kriminalvården opportunity to continuously replace applications as well as to update the infrastructure services without having to make consequential amendments in the applications or the framework.

Another distinctive feature of the architecture is that at least two security domains will be used. In the “Security domain for the offender” the storage of sensitive information is minimized. This information will instead live in the "security domain for administrative applications", where business systems are available. Possibly there may also be a security domain to administer the domain of offenders.

The table below describes the overall requirements of quality attributes for the applications.

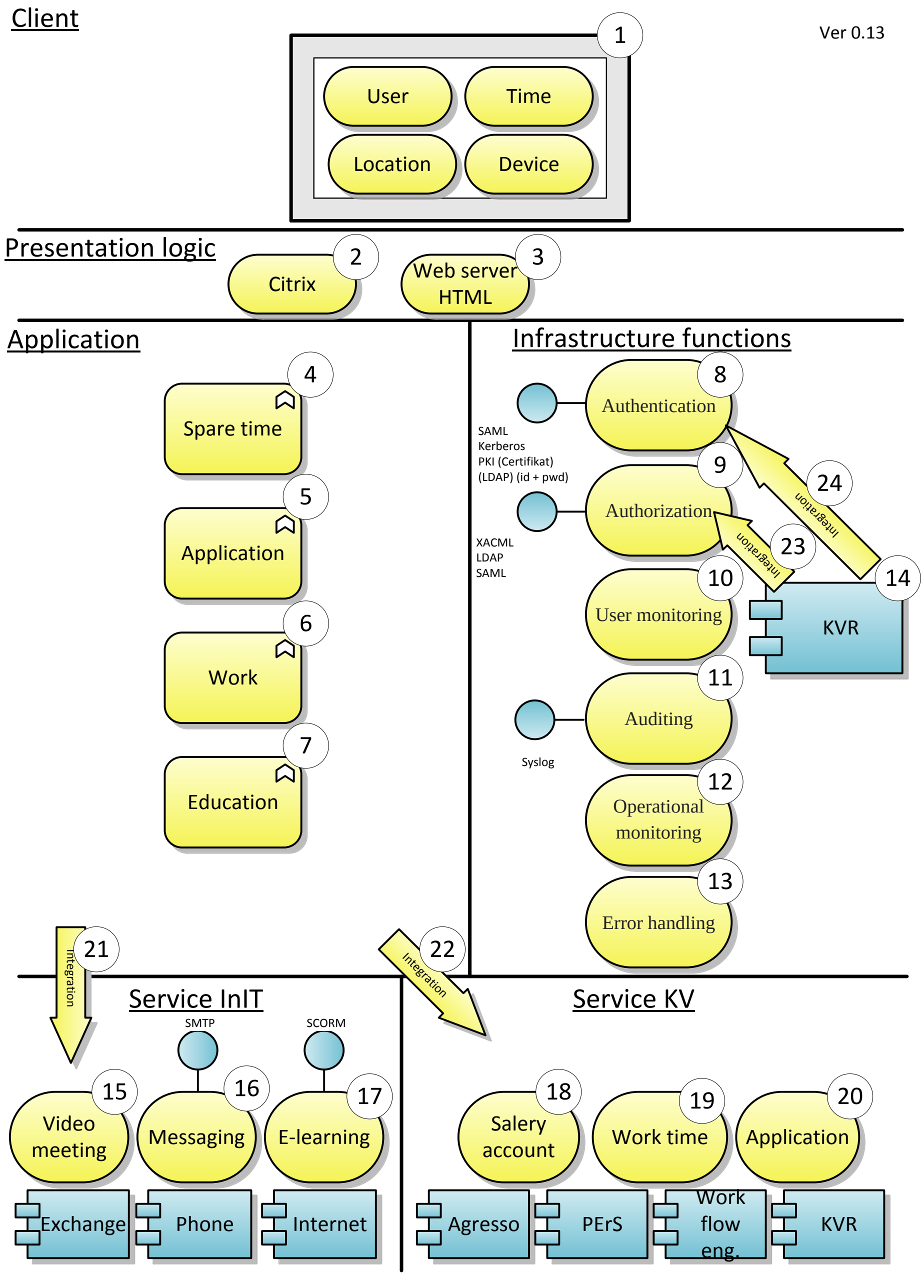
Quality attribut	Requirements
Availability	The platform should be available to the offenders between 6:00 to 01:00 during the week.
Performance	Performance load is highly variable. This means that the performance requirements are not yet specified. The supplier shall present the load put per application on the system in terms such as bandwidth utilization per user.
Testability	The applications should where possible, provide error messages to the operation. Furthermore, it should be possible to continuously monitor response time. Since Kriminalvården aims for high quality and low administration needs, good testability is desirable.
Usability	It should be possible to control the language of labels, dubbing and help texts per-user. It should be possible for the text to be read aloud by the application, i.e. a voice speaking. Furthermore, it should be possible to enlarge the screen for people with visual impairment
Security	* Offenders should under no circumstances be able to, or have the possibilities to continue criminal activities. * Offenders must not be given the opportunity to receive information outside of correctional system control. * Offenders must not be allowed to communicate with others outside of correctional system control, whether inside prison or to parties outside of prison or jail.
Modifiable	It should be possible to make configurations for the relevant functions. The supplier must report what can be controlled with the configuration for the current application.

Figure 2 Quality Attributes

Appendix 1 Infrastructure Services

Below is a description of the framework for IT support to the offenders. The architecturally distinctive needs include the common infrastructure services for:

- Authentication
- Authorization
- Auditing
- User monitoring
- Operational monitoring
- Error handling
- Integration



The purpose of these services is to increase reuse to minimize operating and development costs. Furthermore, these services mean that there should not be separate administrative interfaces for each application. The idea is for example that any authorization administration should be handled from one place. Similarly, all audit logs are collected in one place where analysis can be done.

These services are defined so that the protocols, etc. are encapsulated behind open standards. The list below describes these services.

1 Authentication (8)
Users are registered in an LDAP directory. Login is done using two-factor authentication (e.g. smart card and fingerprint). The technique for authenticating users must not be based on passwords. Single Sign-On (SSO) can be achieved by using SAML.

2 Authorization (9)
A request is made to a centrally managed service for authorization, when the user requests access to function, data, and similar. The request can be made using LDAP, XACML or other general accepted standard.

3 Auditing (11)
Applications and systems software should send log entries with information about what the user is doing. These messages will be escalated according to defined rules. The format of the log entries are syslog or other general accepted standard.

4 User monitoring (10)
User monitoring means that the sessions are recorded and that staff can monitor what the offenders do in the systems. Monitoring should be independent of the display technologies such as HTML and Citrix session.

5 Operational monitoring (12)
Furthermore, it should be possible to receive information about current response times and similar depending on the message generated by the applications.

6 Error Handling (13)
Error handling means that error messages are received from software and applications and escalated according to defined rules.

7 Integration (21, 22, 23, 24)
This functionality means that the transition between two security domains is monitored to ensure that only authorized traffic can pass.

Appendix 2 Applications

The following section describes the applications that can be offered to the offenders. Each application lists the requirements to be answered. It should be noted that certain applications may be offered by another function. Examples of this are the canteen and survey functionality which could conceivably be offered in a CMS.

The applications are:

- Portal
- My Files
- Video On Demand, TV
- Internet access
- Appointment / Calendar
- My Messages
- Internal forms
- Authority contacts / official forms
- Content Management System (CMS)
- Surveys
- Learning Management System (LMS)
- Video and audio conferencing
- Offender Trust Fund
- Storage of personal property
- Notification of illness
- Time tracking
- Canteen
- E-library
- Telephony
- Language support and other aids

1. Portal

The portal is the operator interface from which the offender can be given access to the various applications.

Aspect	Requirements	
Purpose	The purpose of the portal is that the offender will receive information about the applications and information sets that are available. The portal should also serve as a central application for other applications.	
Functionality	The following functions should be available: • Only those applications that the user's privileges allow should be visible. • Information relevant to the user and its location is displayed via a CMS. • Labels and help texts language should be controlled depending on who the user is, through configuration files that allow for external translation	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to this application should be handled by the central authorization service.
	Auditing	It should be possible to log the use of this application.
	User monitoring	It should be possible to record the users' choices.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Not applicable.

Figure 3 Requirements for portal

2. My Files

My files involve the possibility that the offender has to store files. These files may have been copied to or created by the user. In some cases, these files should be read-only.

Aspect	Requirements	
Purpose	The application's purpose is that the offender should be able to store personal files. The files should be handled according to these classifications: • Files that only the offender can handle, including ○ files they can only read ○ files they can modify • Files that also Kriminalvården can handle, including ○ files related to activities ○ personal files	
Functionality	It should be possible to prevent data to be created, write-protect files and limit the file formats that can be stored. Furthermore, the area should be protected against data viruses. The size of the file area should be limited. There will be a limit when the file area can be reached on the basis of date and time of day, as well as of file metadata. Kriminalvården should be able to search the file areas for certain formats, encrypted files and compressed files should be possible.	
Standard	The user interface should be in HTML5 or a file manager.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the central directory service.
	Authorization	Access to this application should be handled by the central authorization service. There may be different access rules for different directories.
	Auditing	It should be possible to log the use of this application.
	User monitoring	It should be possible to generate warning messages regarding usage, for example when the number of files of a certain type exceeds a given level.
	Operational monitoring	Operational errors should be reported, e.g. low disc space.
	Error handling	Errors should be reported.
	Integration between security domains	Not applicable.

3. Video on Demand, TV

This application allows the user to watch streaming media.

Aspect	**Requirements**	
Purpose	It should be possible to select and watch Video on Demand and TV on the offender’s device.	
Functionality	It should be possible to search for movies based on certain search criteria. It should be possible to charge for the opportunity to watch video. These funds shall be taken from the offender's trust fund, see the corresponding section. Where possible, the user should be able to control the language for dubbing and subtitling. Furthermore, it should be possible to select and watch TV. The solution should also keep abreast of how the media is distributed in the network in an efficient way. The bandwidth requirements should be included in the response to the RFI.	
Standard	Support for compression, etc. Administration should be available in HTML5, while the solution can exist as a service within Kriminalvården’s security domain.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	It should be possible to limit the user's ability to watch a defined set of movies and TV channels.
	Auditing	It should be logged what movies the user has watched.
	User monitoring	It should be possible to see what movie the user is watching.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Not applicable.

4. Internet access

This application make is possible for the offenders to access Internet.

Aspect	Requirements	
Purpose		
Functionality	Kriminalvården shall have full control over threats to the mission integrity. Kriminalvården shall be able to efficiently control what web pages the offenders can access. Offenders must under no condition be allowed to communicate through this application, allowing them to continue with criminal activities. Offenders must also not be able to send non-authorized information through the application. Also, download of information shall be under full control by Kriminalvården. Kriminalvården should be able to cache web pages for offline browsing by the offenders. This caching should be completely static.	
Standard	HTTP(S) sessions with HTML including HTML5 should be managed, depending on choice of security solution.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the central directory service.
	Authorization	It should be possible to limit the browsing experience by using white- or blacklists, or through similar measures which also meet the functionality criteria.
	Auditing	Selection of URLs, etc. should be logged.
	User monitoring	All web browsing should be recorded and continually monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	There will be features to prevent unauthorized access from outside through this application.

5. Appointment / Calendar

Technically speaking it can be possible to meet this requirement in the form of an application in a CMS.

Aspect	**Requirements**	
Purpose	The purpose of this application is to allow the user to book gyms, doctors, guidance counselors, etc., and also to provide a tool for overviewing all personal activities.	
Functionality	It should be possible to enter offenders wish to make an appointment. Possibly it should be possible to see what times are available. The user will be able to view a calendar of completed bookings.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user shall be identified according to the function for this.
	Authorization	It should be possible to control the booking types available for the user. Furthermore, it should be possible to restrict access to booking so that the booking must also be approved by the staff.
	Auditing	Completed bookings should be logged.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Some information in the calendar can imported from a different security domain.

6. My Messages

This feature will allow the offender to send messages to predefined recipients.

Aspect	**Requirements**	
Purpose	The offender should be able to send messages to externally defined and approved recipients.	
Functionality	This function should support: • Translation of texts between languages. The supplier shall specify the quality of translation that can be done. • Before a message is sent, Kriminalvården should have the possibility to examine and approve the contents. • Before a message is read by the offender, Kriminalvården should have the possibility to examine and approve the contents. • Approved recipients shall be collected from an external service supplied by Kriminalvården in a format that will be developed jointly with the supplier. The supplier must specify the workflow that supports this functionality.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	It should be possible to configure what persons / functions that the offender can send messages to. It should be possible to control via the contents and recipients of the message whether or not it needs review before the message is delivered or becomes available to the offender.
	Auditing	It should be possible to log sent and received messages.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Messages will be transferred between security domains.

7. Internal forms

This application will allow the offender to fill in certain specific forms for further processing by the staff. A form can for example be a request for leave.

Aspect	**Requirements**	
Purpose	The purpose of this application is to give the offender the option to apply for leave, etc. This is done by filling in predefined forms which is then handled in another Kriminalvården service where decisions are made and administered. The offender can then via this application get information on the current status of the errand or decision result if he or she is authorized to do so. Kriminalvården is responsible for supplying the contents of the forms.	
Functionality	It should be possible to control the language of labels and help texts depending on the offender's language. Types of applications: • Leave • Possession / purchase • Management of storage for personal property • Applying to a substance abuse treatment or personal improvement program The supplier should specify the workflow that supports this functionality. Furthermore, the supplier should also specify if it is possible for the user to add electronic signatures to the form.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to this application should be handled by the central authorization service. Indicating which applications the user may send, who will receive them and how decisions should be communicated to the user.
	Auditing	It should be possible to log sent and received messages.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Applications will be transferred to a different security domain.

8. Authority contacts / official forms

Technically speaking it can be possible to satisfy some of these requirements in the form of an application in a CMS.

Aspect	**Requirements**	
Purpose	The purpose of this function is that the offender should have access to a selection of official forms that he or she can fill in. Depending on how security is set up, the completed form is forwarded to an authority using the messaging function (#6). In this function, there might also be an opportunity to take part of the Authority's website using the internet function (#4). Furthermore, this feature can provide the opportunity for the offender to exchange communication with external agencies if the offender has permission to do so.	
Functionality	This application shall have the following functions: • Access to selected parts of certain government websites. • Access to selected official forms. • Ability to fill out a form. • Ability to save a completed form. • Depending on the authorization, the possibility of exchanging message with an agency.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to this application should be handled by the central authorization service: • Access to function • Ability to save completed forms • Ability to exchange messages with authorities
	Auditing	There should be a record of: • Sent forms • Notices to / from authorities
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Not applicable.

9. Content Management System (CMS)

Using this application, the offender should be able to access information through a Web browser. Further, this application can be used to implement (see section):
- government contacts
- appointment
- survey
- canteen
- notification of illness

Aspect	Requirements	
Purpose	The purpose of the Content Management System (CMS) is to give the offender access to information via a web browser. This information can for example.refer to instructions in working operation and the week's food menu.	
Functionality	The functions of the editors and readers should be very clearly separated e.g. via a front-end and back-end setup. It should be possible to have local and central editors. The CMS should host enough capabilities to include personal/offender specific portals.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to this application should be handled by the central authorization service. E.g. which pages the user has access to read.
	Auditing	It should be possible to log the use of this application.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Not applicable.

10. Surveys

Technically speaking, it may be possible to meet this requirement in the form of an application in a CMS.

Aspect	Requirements	
Purpose	The purpose of this function is to manage forms for follow-up activities. The information in the forms should be analyzed in an analysis function.	
Functionality	The offender should be able to answer surveys. This can e.g. be done by giving a message and / or URL. In the form it should be possible to have different types of questions. The answers can be free text, multiple-choice, scales and one-option choice. The answers are to be analyzed using an analysis tool.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	The ability to see the answers to the tests will be controlled by the central authorization service.
	Auditing	It should be possible to log the use of this application.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Not applicable.

11. Learning Management System (LMS)

Education activities in prisons and remand jails takes place both in physical premises known as learning centers and remotely via electronically distributed materials and electronic communication in the form of forums between teacher and student. A single teacher can have several courses in the same subject at the same level both locally and remotely at the same time. A single teacher can have several courses in various subjects both locally and remotely at the same time.

At some locations, students from different wings aren’t allowed to meet for security reasons. There is thus a need for the application to in a controlled way only allow offenders from the same wing to be scheduled at the same time. There is also a need to limit the admission of certain offenders to certain learning centers depending on the classification. For example, high risk offenders might only be able to visit specific learning centers.

Admissions are perpetually ongoing in the sense that the offenders can apply at anytime and new students are enrolled every week as long as there is a free seat. This function can use:

- My Files
- Internet access
- My Messages

Aspect	**Requirements**
Purpose	The purpose of this application is to administer education and serve as a platform for ongoing education.
Functionality	The purpose of this application is to give offenders the opportunity to study. These studies can be made via: • Educations which are packaged as SCORM • Educations via video sessions where the inclusion of a white board functionality is seen as an advantage. • The teacher and student can send files, message, etc. to each other. • Teaching through access to the HTML-based applications • Teaching through use of Windows-based applications via Desktop Access. The supplier should describe the business processes supported. The following should be administered. However, it may be in a separate application: - Available curriculum - Teacher resources and availability - Enrollment - Scheduling - Attendance registry - Documentation of knowledge according to guidelines for rating requirements

Aspect	**Requirements**	
	- Completed courses - Certificates and proof of completed courses based on configurable templates	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to education is regulated by the central authorization service. The same function will handle the rights of teachers in the application.
	Auditing	It should be possible to log the use of this application.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Not applicable.

12. Video and audio conferencing

Aspect	Requirements	
Purpose	The purpose of this function is that it should be possible to arrange meetings without having to move physically.	
Functionality	This application should support the following types of communication: • Teacher - student, both in InIT • Offender - children, offender from InIT, children via the Internet • Probation officer - offender, both outside InIT • Offender - lawyer, offender within InIT, lawyer outside A session will be monitored (see below). At this monitoring, the sound and / or image can be shut down. Furthermore, it should be possible to pause the session so that the controller can communicate with the attendees. The supplier should specify the requirements for handling video and telephone meetings. Furthermore, the supplier should specify how to safely identify the counterparty, e.g. when using IP telephony. The answer should contain specifications regarding bandwidth needs. The service shall be usable by external parties with minimal technical requirements.	
Standard	The manufacturer should suggest a suitable standard.	
Support to infrastructure components	Authentication	User from InIT should be identified and authenticated using the SSO service. Users outside InIT should be identified using E-ID or an equivalent service.
	Authorization	Possibility of video and teleconference and with whom is handled by the central authorization service.
	Auditing	Logging may be made of the meetings that took place, during what time and with whom.
	User monitoring	The session should be recorded and continuously monitored. Contacts between clients and lawyers will not be monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Not applicable.

13. Offender Trust Fund

This application can be reused by:
- Video on Demand, TV
- Video and audio conferencing
- Canteen
- E-library
- Time tracking
- Internal and external forms

Aspect	**Requirements**	
Purpose	This application relates to the management of the offender trust funds. These are handled by an account into which deposits are made as compensation for work and study. Furthermore, the account can be charged e.g. based on the purchase at the canteen and rented movies.	
Functionality	The application shall support the following processes: • Compensation for time completed within work assignments and studies • Charging the account based on the purchases in the canteen, rented movies, etc. • Ability to see transactions and get information about the balance The supplier should describe how the processes are supported.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	The user's ability to access this feature and to make printouts should be handled by the central authorization service.
	Auditing	Logging may be made of the transactions carried out by whom and when. Furthermore, it should be possible to log who has seen what and which printouts have been made.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	To obtain information about the offender’s trust fund there must be an integration to a different security domain.

14. Management of personal property storage

This application handles the offender’s storage, i.e. physical properties such as watches, clothes, etc.

Aspect	**Requirements**	
Purpose	This application is used to manage the offender’s storage where physical belongings are stored by Kriminalvården.	
Functionality	The following business processes should be supported: • Submission to the store. • Withdrawals from the store. • List the contents of the store. • Function for managing loss from storage. The supplier shall describe the way processes are supported.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	The user's ability to access this feature and to make printouts is handled by the central authorization service.
	Auditing	Logging may be made of the transactions carried out by whom and when. Furthermore, it should be possible to log who has seen what and which printouts have been made.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	To obtain information about the offender’s storage there must be an integration to a different security domain.

15. Notification of illness

This function handles sickness and associated procedures such as medical certificates, etc. This functionality could be implemented in the CMS. Furthermore this also affects compensation calculation. Kriminalvården would also like for the manufacturer to make suggestions regarding processes and functionality based on their experience.

Aspect	**Requirements**	
Purpose	This application will streamline the administration of reporting sickness.	
Functionality	The application should support the following business processes: • Informing staff about being ill • Allow staff to register eventual medical certificates so that these can be attached to a notice of illness. • The application should automatically supply information about sick leave to the offender's trust fund. The supplier should describe the way processes are supported.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to this application should be handled by the central authorization service.
	Auditing	It should be possible to log the use of this application.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Information on reporting illness is transferred to another security domain.

16. Time tracking

This function handles the registration of work and study. This functionality could be implemented in CMS. Furthermore, this can also be integrated with the offender trust fund and Kriminalvården's time management system.

Aspect	**Requirements**	
Purpose	This application will streamline the administration of time tracking as well as give the offender an enhanced digital experience.	
Functionality	The following business processes should be supported: • Register time for when the work / study session was initiated ○ Automated through card reader or other technical solution • Register time for when the work / study session was completed ○ Automated through card reader or other technical solution • View timesheet through standard interface • Correct registered time through an administrative interface with authorization control The supplier should describe the way business processes are supported.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to this application should be handled by the central authorization service.
	Auditing	It should be possible to log the use of this application.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Information about the tracking is transferred to another security domain.

17. Canteen

Technically speaking, it may be possible to meet this requirement in the form of an application in the CMS. Furthermore, integration must be made to the offender’s trust fund. This application consists of an administration section and a user section for offenders. These components should live in two different security domains.

Aspect	**Requirements**	
Purpose	Using this application, offenders can order things from the canteen.	
Functionality	The following business processes should be supported: • List of products • Search for products • Ordering products • Perform payment The supplier should describe the way business processes are supported.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to this application should be handled by the central authorization service. There may be restrictions such as how much fruit that can be purchased.
	Auditing	It should be possible to log the use of this application.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Not applicable.

18. E-library

The purpose of this application is to allow the offender access to different kinds of books. This could be implemented in CMS and have a link to the offender’s trust fund. This application consists of an administration section and a user section for offenders. These components should live in two different security domains.

Aspect	**Requirements**	
Purpose	The purpose of this application is that the offender should be able to access different types of books.	
Functionality	The business processes to be supported are: • List of products • Search for products • Ordering products • Download product • Read / listen product • Perform payment Items that can be borrowed include: • Books • eBooks • Audiobooks • Papers • Music The supplier should describe the way the business processes are supported.	
Standard	The user interface should be in HTML5.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to this application should be handled by the central authorization service.
	Auditing	It should be possible to log the use of this application.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.
	Integration between security domains	Not applicable.

19. Telephony

The purpose of this application is that the offender should be able to receive and make external calls with people outside a prison. Kriminalvården aims with this application to cover functionalities that exists in the current system, INTIK which is used today.
The application should consist of one administration and one user component covering both IP and switched telephony.

- For IP based telephony enabling offenders to make/receive calls from a computer based terminal.
- Switched telephony systems should enable calls to be made through a switched system, but also include administrative tools which allow management according to the infrastructural components described below.

These components should live in two different security domains.

Aspect	**Requirements**	
Purpose	The system for offender's telephony (INTIK) is a system to facilitate and simplify phone calls from offenders and reduce the amount of intercepted calls, increase security, and provides an easy way to manage the service for offender telephony.	
Functionality	The business processes to be supported are: • Calling people according to a list of approved numbers. • Receive calls according to a list of approved numbers. • The system should have security features that blocks attempts to call a third party or use call forwarding. • Verification that calls are made only to authorized numbers. • Ability to record calls. • Logging of all changes made to the system. • Report functionality. • The system should be able to count the time spent in a call and forward cost and time numbers to a centralized system or charge offender's trust fund for the calls cost The supplier should describe the way business processes are supported.	
Standard	The user interface should be in HTML5.and include a suitable solution for managing switched phone calls.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to this application should be handled by the central authorization service.
	Auditing	It should be possible to log the use of this application.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported.
	Error handling	Errors should be reported.

Aspect	**Requirements**	
	Integration between security domains	Not applicable.

20. Language support and aids

The platform should support offenders with disabilities or offenders speaking foreign languages. The purpose of this application is to provide this support to any of the applications previously listed. At the very least this entails having an API where text can be fetched and maybe also read aloud. Kriminalvården is open to further suggestions in this matter.

Aspect	**Requirements**	
Purpose	The purpose of this application is to give other applications the possibility to handle text messages in different languages. Also, offer other utilities to aid the user.	
Functionality	The application should: • Handle different languages • Read text More suggestions from the supplier is welcome.	
Standard	The supplier should suggest a defined API.	
Support to infrastructure components	Authentication	The user should be identified and authenticated using the SSO service.
	Authorization	Access to this application should be handled by the central authorization service.
	Auditing	It should be possible to log the use of this application.
	User monitoring	The session should be recorded and continuously monitored.
	Operational monitoring	Operational errors should be reported
	Error handling	Errors should be reported
	Integration between security domains	Not applicable

Appendix 3 Devices

For offenders to have access to information they need different physical devices. This section describes five types:

- Device for the identification of users
- Device in the living areas
- Device in the learning center and for work assignments
- BBS / kiosk in common areas
- Secure wireless solutions

For some of these devices it should be possible to identify the offenders. The different types of devices are described below.

1. Device for the identification of users

The offenders should be identified by two-factor authentication. Currently there is an ongoing procurement of an identification solution that will be used within Kriminalvården. This concept can also be used also in InIT. The identification solution is a smart card along with fingerprints. The OSS solution should use this authentication mechanism, or provide something equivalent.

Aspect	**Requirements**	
Purpose	The purpose of this device is to positively identify the user.	
Functionality	The device should identify the user by using strong authentication. The supplier should describe how to satisfy these requirements.	
Standard	The user interface will be in HTML5.	
Support to infrastructure components	Authentication	Yes
	Authorization	No
	Auditing	No
	User monitoring	No
	Operational monitoring	No
	Error handling	No
	Integration between security domains	No

2. Device in the living areas

There are about 5000 living quarters at Swedish prisons. These will eventually be fitted with a device so that the user can achieve the above described applications.

Aspect	**Requirements**	
Purpose		
Functionality	Device should comply with requirements such as: • Short cables to reduce risk of suicide • Allow for simple security searches • Not be used as weapons The supplier should describe for how these requirements are met.	
Standard		
Support to infrastructure components	Authentication	Yes
	Authorization	Yes
	Auditing	Yes
	User monitoring	Yes
	Operational monitoring	Yes
	Error handling	Yes
	Integration between security domains	No

3. Device in the learning center and for work assignments

In prisons and some jails there are learning centers where offenders can be given the opportunity to study. In these learning centers there is the opportunity to study with the help of a computer. Furthermore, there are areas for work assignments. These activities sometimes involve the use of computers, for example to gain access to work instructions and safety precautions or to produce design drawings and manage orders and shipments.

Aspect	**Requirements**	
Purpose		
Functionality		
Standard		
Support to infrastructure components	Authentication	Yes
	Authorization	Yes
	Auditing	Yes
	User monitoring	Yes
	Operational monitoring	Yes
	Error handling	Yes
	Integration between security domains	No

4. BBS / kiosk in common areas

In public places there may be electronic bulletin boards or kiosks where an offender can get access to information.

Aspect	**Requirements**	
Purpose	The purpose of the kiosk is to give the offender easy access to information.	
Functionality	The kiosk should have the following functionality: • Via the touch screen should be able to choose functionality. • It should be possible to connect equipment for the identification of users (see "1 Device for identifying user").	
Standard		
Support to infrastructure components	Authentication	Yes
	Authorization	Yes
	Auditing	Yes
	User monitoring	Yes
	Operational monitoring	Yes
	Error handling	Yes
	Integration between security domains	No

5. Secure wireless solutions

Aspect	Requirements	
Purpose	The aim is to enable secure wireless access primarily for tablets and mobile phones.	
Functionality	The supplier should describe how to satisfy the following requirements: • Describe encryption solution, incl. supported algorithms and key lengths. • Describe support for 802.1x certificate authentication for LAN as well as WLAN. Should also support authentication based on the MAC address for the equipment that do not have 802.1x support. • Tool and / or concepts and ideas such as ARP cache protection, to protect against ARP cache poisoning / ARP spoofing but also against "rouge AP". • Upgrades of algorithms, key lengths and techniques should be possible, simple and safe. • Process for certificate and key management and updating. • Intrusion detection of unauthorized clients and unauthorized wireless networks.	
Standard		
Support to infrastructure components	Authentication	Using certificates
	Authorization	For example, can be a need to give different users different access opportunities.
	Auditing	Successful and unsuccessful logins will be described.
	User monitoring	No
	Operational monitoring	Yes
	Error handling	Yes
	Integration between security domains	No