Cyber-Authentication

Architecture and Specification
August 2009

Table of Contents

Executive Summary

The Crown requires an open, risk-based strong authentication platform that enables departments and organizations to layer security across diverse users, transactions and applications, applying the right level of authentication tailored to the risk associated with actions that a user is performing. For flexibility, the Crown needs a range of authentication capabilities including NIST–approved L2 and L3 credentials. This allows Departments the flexibility to match the authentication method based on user experience, security requirements and cost, rather than being tied to one single authenticator. Authentication can optionally require direct user interaction (tokens, grid, one-time-password) or can be transparent to the user (machine authentication or IP-Geolocation).

The required platform must offer:

Flexible Security

- The platform must offer user name and password as an authentication baseline, but must provide options for strong authentication which increase the security of online identities significantly and reduces the risks associated with password only authentication.
- The flexibility of multiple credentials, enabling departments and organizations to layer the credentials for maximum security and authentication.
- The platform will offer mutual authentication for the increased security of both the citizen and the Departments to ensure they are both dealing with the other (not just departmental auth of the citizen).

Ease of Integration

The platform must:

- Work in a Department's environment with minimal impact to existing infrastructures, including existing authentication applications, web access control platforms and user repositories.
- Have easy administration with centralized Web-based tools.
- Be highly scalable to help meet the availability and service level requirements of a wide range of applications.
- Offer standards-based API's (ex: Web services, Radius) for ease of integration with internal and external 3rd party systems.

Cost Reductions

The platform must:

- Enable the implementation of a range of strong authentication capabilities at very low cost. There must be no singular requirement for specialized authentication hardware.
- Be hardware independent, to make the platform highly portable and convenient to the end user. The platform must be supported on Windows, UNIX, Linux, and AIX platforms.

- Offer a robust, simple and centralized platform for authentication, ensuring that the Departmental deployment is swift and cost-effective.
- Include a Self Service capability to enable users to self register and administer their accounts, reducing the amount of demand placed on the help desk and increasing overall user satisfaction with government services.

1 Technical Requirements

The Crown has defined the following technical requirements.

1.1 Platform Capabilities

At service delivery – expected October 2010 - the following capabilities must be a part of the system platform:

- Liberty SAML v 2.0 approval for federated services (IDP)
- Wide range of authentication capabilities, including username and password for primary authentication, as well as a range of strong authentication capabilities, including specifically:
    - Various non-invasive authentication capabilities (ex: IP-Geolocation, Device authentication, Questions and Answers)
    - Various non-physical second factor authentication capabilities (ex: eGrid, out-of-band OTP soft token)
    - PKI Certificate authentication support as a COTS option in the system
    - The ability to add new authenticators easily through standards such as PSKC and OATH
    - Transaction digital signatures for increased confidence in online transactions
    - Role-based Web Administration system
    - Administrative reporting
    - Easy integration via standards such as Web services and/or Radius

1.2 Platform Architecture

The ideal platform will be a versatile authentication server that provides numerous authentication methods to applications using a single administrative and policy based engine. It must be engineered to leverage existing identity stores (i.e. LDAP, RDBMS) found within the Department's environment where user information is already present. The platform must utilize existing LDAP or Active Directory entries to store its authentication information. This approach reduces the need to synchronize user data between identity stores and leverages existing High Availability and Disaster Recovery schemes already in place. If the first factor information is not present in a LDAP like system, the platform must be able to leverage the existing database servers (i.e. MSSQL) to store the authentication information.

The proposed architecture to be deployed as an enterprise-wide platform will offer username and password for primary and options for L2 and L3 strong authentication for various user scenarios that can include authentication to a Government Department as part of a Canadian Government web application. The platform components will include:

- Versatile authentication server
- Government of Canada Auth DB

- Liberty Certified Federation infrastructure
- Government of Canada web applications
- Third Party web applications
- The deployed solution will include the following capabilities:
    - The versatile authentication server platform will offer web services and Radius interfaces that will enable strong authentication to Government of Canada web applications. The strong authentication capabilities will leverage the exiting authentication with the GC Auth DB.
    - Users will be authenticated only upon successfully entering existing authentication and (optional) successful additional strong authentication.
    - The platform will also leverage the Federation Infrastructure. Users that are trusted by third party applications using the Federation Service (SAML) will be authenticated to the Government of Canada application.
    - Authenticated users will be authenticated to third party applications using the same Federation Service.

1.3 Liberty Alliance SAML v2.0 Compliancy

The platform must be viewed as Liberty Alliance compliance for SAML 2.0 compliance upon production start date.

1.4 NIST Assurance Level 2

The platform must have COTS options for NIST approved Level 2 compensating factors such as IP GEO location, Knowledge questions, and device authentication without need for integration with additional third party products.

1.5 NIST Assurance Level 3

The platform must have COTS options for NIST approved Level 3 authentication factors such as using Grid or SMS/email messaging or One Time Password (OTP) tokens, and PKI certificate authentication without need for integration with additional third party products.

1.6 NIST Assurance Level 4

The platform must have COTS options for NIST approved Level 4 authentication factors such as a PKI certificate.

1.7 Configuration Management

The platform must be able to be routinely installed by customer IT departments within a 48 hour period and must be able to be configured to handle High Availability deployment options.

1.8 Credential Management

The platform must have a centralized self service capability that handles user login, self registration, self administration and password management. This must be COTS and not require extensive configuration or customization.

1.9 Audit Logging

The platform must provide logging and auditing capabilities whereby all activities, whether user or administrative, are tracked. The audit information should be a configurable a recording of day-to-day operations which can be sent to syslog, remote syslog, a text file, or a database.

The auditing level must be able to be changed depending upon the amount of details required.

1.10 Reporting

The proposed platform must provide logging and auditing capabilities whereby all activities, whether user or administrative, are tracked. The solution must include built-in reporting and querying capabilities to facilitate an understanding of the user community's behaviour at any given time. In addition, external standard reporting packages, such as Cognos Reportnet or Crystal Reports, must be able to be leveraged to generate reports on activities.

1.11 Bench Tested Scalability

Based on a total authentication response time (challenge plus response) of 300 milliseconds or less and all servers running at 50% Computer Processing Utilization (CPU), the platform must be able to process 150 authentications per second or better on reasonable hardware (ex: Intel-based hardware). An example of a system that should be able to perform to this level is:

- Running on IBM xSeries 336 servers with Dual Xeon 3.2 GHz CPU and 2GB memory
- Hyperthreading set to "on"
- Running on Windows Server 2003 and Red Hat Enterprise Linux AS 5 operating systems
- Interacting with either LDAP Directory and database repositories

2 Integration

2.1 Self-Serve Workflow

The self service option must allow users to perform specific administrative tasks that are controlled by administration policy. Tasks vary and are dependant on the configuration and authenticators deployed.

Self Registration tasks must include configurable abilities such as:

- Choosing a mutual authentication image
- Entering a mutual authentication phrase
- Choosing questions and entering answers for knowledge based question and answer authentication
- Entering contact information (either email addresses or telephone numbers or both) for use in sending one-time passwords for out-of-band authentication
- Registering for a physical second factor of authentication, including grid, token or both
- Creating a password
- Associating an existing X.509 digital certificate with a user

Self Administration tasks (once registered) must include configurable capabilities such as:

- Changing or recovering a password
- Changing or adding contact information
- Changing mutual authentication images or captions
- Changing questions and answers for knowledge based question and answer authentication
- Managing devices authorized for a user, including adding a new one or removing an existing device
- Requesting a new grid or token
- Activating a new grid or token
- Reporting a token lost or found
- Unlocking a challenge response token
- Creating or recovering a personal verification number (PVN)
- Requesting a temporary PVN
- Associating a new X.509 digital certificate with a user and/or removing one

2.2 Credential Lockout

The platform must include the ability to lockout a credential. This ability must be controlled by policies regarding the number of attempts before lockout and lockout period or lockout action. Policies must be able to be configured based on groups of users as well as an entire user population.

2.3 Credential Password Recovery

The self service capability set must enable users to manage their passwords.

2.4 Meaningless But Unique Identifier (MBUN) Support

The platform must not restrict the characters that are allowed and supported for the “userid”. Many operating systems and repositories (SQL and LDAP) do have restricted characters, which the platform will need to follow. Overall the use of MBUNS must be completely supported.

2.5 Validation Rules

The platforms must provide a centralized, robust policy engine. Through policy, Departments must be capable of setting password policies with control over the following:

- Minimum password length
- Password lifetime
- Number of passwords kept in the password history list
- Must include a number
- Must include an uppercase
- Must include a lowercase
- Must include a non-alphanumeric
- The password policy must be allowed to be unique for different user groups

2.6 Multi-language Support

The web pages for user authentication must be setup and configured to fully support CLF2, CLF3 and a language toggle by the Government of Canada department citizens’ facing applications. The use of a SAML authentication must not change or impact the user visible GUI or language.

The platforms browser based administration must be bilingual but it is acceptable if available in English only.

The platforms self service capability must be easily translated to other languages. Support for CLF and language toggling must be evident.

2.7 Multi-tenant Capabilities

The platform must support the ability to have different tenants (or Departments) by the implementations of multiple repositories, multiple groups and partitions.

Each Department can have its own applications and web pages that can all simultaneously interact with the platform to provide the required SAML response(s) and authentication. All interactions with applications must be provided using SSL-protected web services or Radius, allowing service providers to support different tenants in their own web farm while having the central platform server provide a secure authentication response.

2.8 Operating System Interoperability

The platform must be supported on the following operating systems:

- Linux Red Hat Enterprise 4 or 5 (AS/ES editions)
- Sun Solaris 9 or 10
- Microsoft Windows Server 2003 or 2008
- AIX 5.3

2.9 Application Server Interoperability

The platform must be able to support the following application servers in at least one specific combination with an operating system:

- TomCat
- BEA WebLogic 10g R3
- WebSphere 6.1

2.10 LDAP Directory Interoperability

The platform must support a wide variety of directory technologies to meet the requirements of the Crown. The platform must perform all directory interfaces using the industry standard LDAP interface. The following is the list of directories the platform must support:

- Novell eDirectory 8.7, 8.8 SP3
- Critical Path 4.2
- SUNONE 5.2 Patch 6
- IBM Tivoli Directory 6.0, 6.1
- Oracle Internet Directory 10g R2 (with patches), 10g R3
- Microsoft Active Directory 2003, 2008
- Active Directory Application Mode 2003
- Active Directory Lightweight Directory Services 2008
- OpenLDAP 2.4 (2.4.11)

2.11 Database Interoperability

The platform must support a wide variety of database technologies to meet the requirements of the Crown. The platform must perform all database interfaces using the industry standard RDBMS method. The following is the list of databases the platform must support:

- Oracle 9i, 10g R2 Patch set 1 (10.1.4.2), 11g
- IBM DB2 Universal v8.2, v9.0, v9.5
- MSSQL Server 2005,
- MySQL 5.0
- PostgreSQL 8.3.x

3 Performance

3.1 Demonstrated Reliability/Availability

The platform must offer a failover scheme to ensure there are backup systems in place in the event that a primary system fails. This scheme must address high availability and disaster recovery issues including:

- Platform failover
- Directory failover
- Database failover
- Radius server failover

3.2 Demonstrated Relevant Experience

To prove scalability and technical viability, the technology platform proposed must be able to reference two separate customer installations in the public or private sector where deployment levels have reached more than 200,000 users on this technology.

4 Proven Technology Migration Skills

4.1 PKI Migration Skills

Since the platform will require a migration of millions of user IDs off of the current platform (Entrust TruePass Roaming), the vendor must demonstrate proven technical skills in Entrust TruePass. The vendor must provide two customer reference examples where they have deployed TruePass to over 50,000 users or migrated a customer off of the Entrust TruePass platform of similar size onto a new technology platform.

5 Support

5.1 Technical Support Capabilities

The Departments must be able to receive the following technical support:

- Anytime, anywhere access to Online support, via a self-service portal and extensive online knowledge base.
- Comprehensive technical response from security experts, including problem replatform and recovery advice for production and development systems in supported configurations.
- Access to new releases of software products for additional functionality, improved robustness and support for integration with third party products.
- Availability of software patches and product upgrades, including e-mail notification of service packs.
- Personal support management from a dedicated Customer Relationship Manager who provides a single point of contact to manage overall support and platform migration needs.
- Troubleshooting assistance with respect to installation and upgrade of software, planning of security architectures, development of applications using APIs and integration of software with third-party products.
- Proactive support through notification of security bulletins, current known issues and new service packs.
- Efficient electronic download of products.
- Invitations to technical web seminars about frequent service requests and products.
- Notification Service, an email news service that delivers customer support information to its users. This service keeps customers up to date on new products, service packs and patches, documentation and other support information.

5.2 Technical Support Options

The vendor providing the versatile authentication solution must be able to provide a range of support options that can be tailored to the Crown or a particular Department. This includes, at a minimum, the following options:

Service Type	Platinum Key	Gold Key	Silver Key
Emergency Support Hours	7 days a week 24 hours a day	7 days a week 24 hours a day	7 days a week 24 hours a day
Basic Support for North American Customers	7 days a week 24 hours a day	5 days a week 24 hours a day *	8 AM to 8 PM (EST) Monday to Friday
Basic Support for European Customers	7 days a week 24 hours a day	5 days a week 24 hours a day *	7 AM to 7PM (GMT) Monday to Friday
Mutually Defined Trouble Priority	YES	YES	YES
Software Maintenance Releases	YES	YES	YES
Access to Support Portal	YES	YES	YES
Early Notification of Significant Technical Bulletins	YES	YES	YES
Training** • Requirements Definition • 5 days no charge Training	YES	YES	NO
Toolkit Support Discounts	YES	YES	NO

* Midnight Sunday to midnight Friday EST

** Based on eligibility

5.3 Technical Support Escalations

There must be clear definitions of severity levels for problems that may arise with its platform and have well defined support and escalation levels, in line with the Software Support Agreement.

Below is a table providing the definition of severity levels.

Severity Levels	
Level	**Description**
1	Critical errors that completely disable the product and for which no workaround exists on production systems.
2	Either a critical error for which a workaround exists or a non-critical error that significantly affects the functionality of the product on production systems.
3	Isolated error that does not significantly affect the functionality of the product, a benign error or product enhancement request.

Once severity has been assigned to an issue, an agent will refer to the following chart for replatform targets.

Escalation Timing					
Level	**Replatform Target ***	**Level 2**	**Level 3**	**Level 4**	**Level 5**
1	48 hours**	60 minutes	2 hours	4 hours	8 hours
2	5 business days	2 hours	4 hours	8 hours	24 hours
3	15 business days	1 business day	2 business days	5 business days	As required
*** For issues that do not require code changes ** For Silver level support, 24 hour replatform for Platinum and Gold.**					

Note: All timings are in business minutes/hours/days and represent the age of the issue from notification.