



Information Technology Security Guideline

User Authentication Guidance for IT Systems

ITSG-31

March 2009

March 2009



This page intentionally left blank



Foreword

The *User Authentication Guidance for IT Systems* is an *UNCLASSIFIED* publication, issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSEC.

Requests for additional copies or changes in distribution should be directed to your Client Services Representative at CSEC.

For further information, please contact CSEC's ITS Client Services area by e-mail at client.svcs@cse-cst.gc.ca or call (613) 991-7600.

Effective Date

This publication takes effect on April 1st 2009

Gwen Beauchemin
Director, Mission Management

© Government of Canada, Communications Security Establishment Canada 2009

It is not permissible to make copies or extracts from this publication without the written consent of CSEC.



This page intentionally left blank.



This page intentionally left blank.



Table of Contents

Foreword.....	i
Effective Date	i
Revision History.....	iii
Table of Contents.....	v
List of Tables.....	vii
List of Abbreviations and Acronyms.....	vii
1 Introduction	1
1.1 Purpose.....	1
1.2 Audience	1
1.3 Scope	1
1.4 Key References.....	1
2 Designing a User Authentication Solution.....	3
2.1 Authentication Robustness.....	3
2.2 Authentication Design Categories and Requirements	3
2.2.1 Authentication Factors	4
2.2.2 Authentication Tokens	5
2.2.3 Threat Mitigation	7
2.2.4 Cryptographic Module Validation	8
2.2.5 Event Logging.....	9
2.3 Security Assurance	10
2.3.1 Level 1	10
2.3.2 Level 2	10
2.3.3 Level 3	10
2.3.4 Level 4	11
3 References.....	15



This page intentionally left blank.



List of Tables

Table 1. Authentication Solution Design Requirements 13

List of Abbreviations and Acronyms

BSA	Baseline Security Architecture
CSEC	Communication Security Establishment Canada
COMSEC	Communications Security
ESA	Enterprise Security Architecture
FIPS	Federal Information Processing Standard
GC	Government of Canada
IT	Information Technology
NIST	National Institute of Standards and Technology
PoP	Proof of possession
RL	Robustness Level
SAL	Security Assurance Level
TBS	Treasury Board of Canada Secretariat



This page intentionally left blank.



1 Introduction

Critical elements of the design for any IT infrastructure are the security controls used to protect the business process. A security architecture is used to provide a comprehensive structure for the security controls.

A security architecture is comprised of both technical and operational security controls. Technical security controls are focused on security safeguards executed by a computer system whereas operational security controls are implemented and executed mainly by people (as opposed to systems) or techniques. For more information on the baseline structure for a security architecture, refer to the Communications Security Establishment Canada (CSEC) *Baseline Security Architecture (BSA) for IT Systems* [Reference 1]. Authentication is one of the core technical security controls defined in the BSA.

1.1 Purpose

The purpose of this document is to assist with the design and selection of appropriate solutions for users authenticating to a controlled business process.

1.2 Audience

This document is intended for GC departmental IT security coordinators and security practitioners.

1.3 Scope

The scope of this document is limited to providing guidance on the design and selection of user authentication solutions.

This guidance is applicable to user authentication solutions for IT systems in the unclassified and protected domains that require controlled user access. IT systems in the classified domains may require additional design considerations that are not within the scope of this document.

1.4 Key References

This document is based on the research conducted under the CSE Enterprise Security Architecture (ESA) initiative and the NIST *Electronic Authentication Guideline* [Reference 2].

The technical guidance in this publication complements the Treasury Board of Canada Secretariat (TBS) *Guideline on Authentication* [Reference 3] which is used to assist GC program business owners in determining what target level of authentication assurance they require before designing the technical solution.

Detailed background information on the components of an authentication system, the threats that they face, and constraints on the use of authentication tokens is provided in *Technical Addendum – User Authentication Guidance for IT Systems* [Reference 4].



This page intentionally left blank.



2 Designing a User Authentication Solution

This section provides technical guidance on the design and selection of a user authentication solution. To more fully specify requirements for security controls, a robustness model has been developed by CSEC and documented in the *Baseline Security Architecture for IT Systems (ITSG-30)* [Reference 1].

The robustness model described there is an approach for determining recommended robustness levels of security controls based on the business assets values and business objectives (impacts) to be protected and the threat environment.

2.1 Authentication Robustness

The guidance in this document is based on a multi-level robustness scheme comprised of four levels of increasing robustness (Level 1 to Level 4). The authentication robustness levels are suitable for different categories of on-line transactions. In general, transactions where the impact (i.e., level of loss, damage, or harm) resulting from a failure in the authentication security control is low, will require a lower robustness level. Conversely, transactions where the impact is greater will require higher levels of robustness.

Within the context of this document, robustness is characterized by two components:

- a. **Strength of mechanism**. Specifies the strength of the authentication mechanisms; and
- b. **Security assurance**. Provides a measure of confidence in the ability of the authentication mechanisms to appropriately meet its security objectives.¹

The mechanisms (types of solutions within the authentication design requirement categories) and security assurance requirements for the authentication solution are described in **Section 2.2** and **Section 2.3**, respectively.

2.2 Authentication Design Categories and Requirements

This section specifies the requirements for designing an authentication solution at each level of robustness. The selection of an authentication solution at any level of robustness is based upon satisfying the requirements from all five of the following authentication design requirement categories:

- a. **Authentication Factors**. Defines how many authentication factors are required during the authentication process (e.g., one factor, two factor, or multi-factor);
- b. **Authentication Tokens**. Defines which tokens are to be used to perform the authentication process (e.g., password, soft token, or hard token);
- c. **Cryptographic Module Validation**. Defines the level of validation that is required for a cryptographic module-based token;

¹ CNSS National Information Assurance (IA) Glossary [Reference 5].



User Authentication Guidance for IT Systems (ITSG-31)

- d. **Threat Mitigation.** Defines the threats which the authentication process must be capable of protecting against (password guessing, replay, eavesdropping, verifier impersonation/phishing, man-in-the-middle, session hijacking);
- e. **Event Logging.** Defines the properties of event logging (e.g., level of detail or audit data protection) required during the authentication process in order to maintain the chain of evidence.

These authentication design requirement categories are described in the following sections with requirements specified at each level of robustness. These authentication design requirement categories are also described in detail in *Technical Addendum – User Authentication Guidance for IT Systems* [Reference 4].

2.2.1 Authentication Factors

This section briefly describes the three classes of authentication factors and specifies requirements for them at each level of robustness.

Authentication factors fall into one of the following classes:

- a. ***Something the user knows.*** This represents information of which only the legitimate user should have knowledge (e.g., a password);
- b. ***Something the user has.*** This represents a physical object, which is not trivial to duplicate, over which only the legitimate user has possession and control (e.g., hardware token); or
- c. ***Something the user is or does.*** This represents a physical attribute which is unique to each user (e.g., fingerprint, retina, face, voice, or signature).

2.2.1.1 Level 1

At Level 1, a single factor of authentication is acceptable and sufficient to provide the required level of robustness.

2.2.1.2 Level 2

At Level 2, a single factor of authentication is acceptable and sufficient to provide the required level of robustness.

However, *Something the user is or does* is to be used only in conjunction with a second factor.

2.2.1.3 Level 3

At Level 3, it is required that at least two-factor authentication be used. The second factor of authentication is intended to provide a more secure solution that mitigates the additional threats at this level. The two factors of authentication cannot be of the same type. Furthermore, one of the factors must be *Something the user has*.



User Authentication Guidance for IT Systems (ITSG-31)

The acceptable solutions at Level 3 include the following combinations of authentication factors:

- a. *Something the user has AND Something the user knows*; or
- b. *Something the user has AND Something the user is or does*.

The combination of *Something the user knows AND Something the user is or does* is not considered an acceptable solution.

2.2.1.4 Level 4

At Level 4, it is required that at least two-factor authentication be used. As with Level 3, the second factor of authentication is intended to provide a more secure solution that mitigates the threats at this level. The two factors of authentication cannot be of the same type. Furthermore, one of the factors must be *Something the user has*.

The acceptable solutions at Level 4 include the following combinations of authentication factors:

- a. *Something the user has AND Something the user knows*; or
- b. *Something the user has AND Something the user is or does*.

The combination of *Something the user knows AND Something the user is or does* is not considered an acceptable solution.

2.2.2 Authentication Tokens

Authentication tokens are something a user knows, possesses, or controls that may be used to authenticate a user's claim. This section briefly describes several tokens used for authentication and specifies requirements for them at each level of robustness. Each token falls into one of the three categories of authentication factors described in **Section 2.2.1**.

The authentication tokens considered in this authentication design requirements category are:

- a. **Password token**. A password is a secret that a user memorizes or otherwise keeps secret and should be known only to them;
- b. **Pre-registered secret token**. A pre-registered secret token is a set of challenges and responses that the user establishes during the registration process;
- c. **Look-up secret token**. Look-up secret tokens, commonly implemented as grid cards or "bingo cards", are matrices (electronic or printed) from which passwords are generated via a challenge-response mechanism each time an authentication is required;
- d. **Out-of-band secret token**. An out-of-band secret token is a combination of a physical device (e.g., pager, cell phone, PDA, land line telephone) and a secret that is transmitted to the device by a verifier each time an authentication is required.
- e. **One-time password token**. A one-time password token is a hardware device that cryptographically generates a one-time password shared between the user and verifier each time an authentication is required;



User Authentication Guidance for IT Systems (ITSG-31)

- f. **Biometric token.** A biometric is a representation of an attribute of a user that can be quantitatively measured and compared against a stored value (e.g., fingerprint, retinal image, facial image, voice pattern, or signature);
- g. **Soft crypto token.** A software crypto token is a cryptographic key that is typically stored on disk or some other storage medium and can be unlocked only with activation data (e.g., password); and
- h. **Hard crypto token.** A hardware crypto token is a device that contains a protected cryptographic key and can be unlocked only with activation data (e.g., password, biometric).

Note: The applicability of a printed look-up secret token (such as a printed grid card) as *Something the user has* (refer to **Section 2.2.1**) is dependent on the specific environment in which it is used and how it is secured and controlled, since a printed token may be susceptible to undetected duplication.

Note: A locally-stored soft crypto token may be susceptible to copying if poorly secured. Additionally, a remotely-stored soft crypto token may not be considered as a factor of authentication, depending on the specific environment in which it is used and how it is secured and controlled.

2.2.2.1 Level 1

At Level 1, the use of any of the authentication tokens is acceptable.

Successful authentication requires that the user prove through a secure authentication protocol that they actually control the token.

2.2.2.2 Level 2

At Level 2, similar to Level 1, any of the authentication tokens may be used.

Successful authentication requires that the user prove through a secure authentication protocol that they actually control the token.

2.2.2.3 Level 3

At Level 3, look-up secret tokens, soft crypto tokens, out-of-band secret tokens, one-time password tokens, or hardware crypto tokens, in combination with another token (of a different factor type) may be used.

If a biometric token is used, its use is restricted to unlocking another authentication token (e.g., unlocking a cryptographic key stored in software or hardware).

Successful authentication at this level requires that the user prove through a secure authentication protocol that they actually control the token.



2.2.2.4 Level 4

Level 4 is intended to provide the highest practical authentication robustness. It is required that users possess a key stored in a hard cryptographic token and use a password or biometric to activate it.

Authentication at this level is based on proof of possession (PoP) of a key through a cryptographic protocol. Successful authentication requires that the user prove through a secure authentication protocol that they actually control the hard crypto token.

2.2.3 Threat Mitigation

Any government computer system is subject to a broad range of threats and attack scenarios. An authentication solution must be capable of mitigating against a set of authentication threats. This section briefly describes several types of authentication threats and specifies requirements for threat mitigation at each level of robustness.

The authentication threats considered in this authentication design requirements category are as follows:

- a. **Online guessing.** In an online guessing attack, an unauthorized party connects to the verifier online and attempts to guess a secret token (e.g., password) with the goal of posing as the legitimate user;
- b. **Replay.** A replay attack is a specific form of man-in-the-middle attack in which an attacker records and replays some part of a previous successful authentication protocol transaction to the verifier in order to gain access to sensitive user data;
- c. **Eavesdropping.** An eavesdropping attack occurs when an unauthorized party listens to conversations between authorized parties (e.g., users and verifiers) and collects their data. Eavesdroppers may listen passively to the authentication protocol exchange and then attempt to learn secrets (e.g., passwords or keys) to pose as legitimate users;
- d. **Session Hijacking.** Session hijacking is a security attack on a user session where an attacker attempts to take over application user sessions. Session hijacking works by taking advantage of the fact that communications may be protected through an initial authentication transaction at session setup, but not thereafter.
- e. **Verifier impersonation/Phishing.** In a verifier impersonation/phishing attack, an attacker poses as the verifier in an attempt to fool a user into divulging secrets; and
- f. **Man-in-the-Middle.** In a man-in-the-middle attack, an attacker places itself in the communication channel between the user and verifier or relying party such that all communications go through it. An attacker may operate in passive mode (collecting information as it relays the data as intended) or may play an active role (communicating with both user and verifier or relying party and impersonating one to the other) to gain access to sensitive user data;



2.2.3.1 Level 1

Level 1 requires that the authentication system be able to mitigate a subset of the documented authentication threats. It is required that an authentication system at this level be capable of mitigating online password guessing and replay attacks.

2.2.3.2 Level 2

Level 2 requires that the authentication system be capable of mitigating a subset of the documented authentication threats. It is required that an authentication system at this level be capable of mitigating online password guessing, replay, eavesdropping, and session hijacking.

2.2.3.3 Level 3

Level 3 requires that the authentication system be capable of mitigating all of the documented authentication threats. It is required that an authentication system at this level be capable of mitigating online password guessing, replay, eavesdropping, session hijacking, verifier impersonation/phishing, and man-in-the-middle attacks.

2.2.3.4 Level 4

Level 4 requires that the authentication system be capable of mitigating all the documented authentication threats. In common with the threat mitigation requirements for Level 3, it is required that an authentication system at this level be capable of mitigating online password guessing, replay, eavesdropping, session hijacking, verifier impersonation/phishing, and man-in-the-middle attacks.

2.2.4 Cryptographic Module Validation

The tokens selected for an authentication system may require the use of cryptographic modules, either in software or hardware. As such, there may be requirements for FIPS 140-2 validation². If no cryptographic module is used, the cryptographic module validation requirements do not apply.

FIPS-validated products (by themselves) are not appropriate for the protection of Classified information. As they become available for the Government of Canada, Type 1 or Type 2 cryptographic module products may be used. These types of products are not FIPS-validated but are appropriate for use at the highest robustness levels for Classified information.

This section specifies requirements for cryptographic module validation at each level of robustness.

2.2.4.1 Level 1

At Level 1, there are no requirements for validation of the cryptomodule.

² CSEC and NIST have issued a draft update to FIPS 140-2. The FIPS 140-3 draft adds an additional security level and incorporates extended and new security features that reflect recent advances in technology.



2.2.4.2 Level 2

At Level 2, there are no requirements for validation of the cryptomodule.

2.2.4.3 Level 3

At Level 3, cryptographic modules implemented in software or hardware are allowed. At least a FIPS 140-2 level 1 rating overall, enhanced with a FIPS 140-2 level 2 rating for identity-based user authentication, for either software or hardware cryptographic modules is required.

2.2.4.4 Level 4

At Level 4, only cryptographic modules implemented in hardware are allowed. At least a FIPS 140-2 Level 2 rating overall, enhanced with a FIPS 140-2 level 3 rating for physical security, for hardware-only cryptographic modules is required.

2.2.5 Event Logging

It is not only important to authenticate users, but it is also necessary to be able to prove that the authentication has successfully taken place or has failed for some reason. In this case, data transferred from the user to the department or agency may need to be captured in some way for evidentiary purposes, such as chain-of-evidence or non-repudiation. Moreover, departments and agencies will need to comply with any applicable policies regarding the retention of event log data for purposes of archival or access. This document, however, does not state requirements on data retention.

Depending on the use of the electronic credentials with the departmental service and the level of risk associated to the online transactions to be undertaken, the exact date and time relating to the authentication may need to be logged. In addition, for added security, the logs can be digitally signed. Depending on the authentication method, traceability may be inherent (e.g., in the case of digital signatures) or may only be achieved by the mechanism through additional manual actions.

This section specifies requirements for event logging at each level of robustness. The requirements for authentication event logging include requirements on the following:

- a. Data that is recorded; and
- b. Protection on the logged data.

2.2.5.1 Level 1

At Level 1, given the low value or sensitivity of the transactions involved, there are no requirements on logging of authentication transactions.

2.2.5.2 Level 2

At Level 2, only simple logging of authentication transactions is required. The authentication mechanism should allow the department or agency to trace the authentication procedure back to



a specific user along with the authentication result and the time it occurred. As well, the event log is protected with some form of access control to limit access only to those who require it.

2.2.5.3 Level 3

At Level 3, logging of authentication transactions, combined with enhanced security is required. The authentication mechanism should allow the department or agency to trace the authentication procedure back to a specific user along with the authentication result and the time it occurred. As well, the event log is further protected with access controls and a tamper-detection mechanism to detect unauthorized modifications to the event log data (e.g., using digital signatures).

2.2.5.4 Level 4

At Level 4, logging of authentication transactions, combined with a high level of security is required. The authentication mechanism should allow the department or agency to trace the authentication procedure back to a specific user along with the authentication result and the time it occurred. The event log is protected with access controls to limit access, a tamper-detection mechanism to detect unauthorized modifications to the event log data, and a tamper-prevention mechanism (e.g., write-once media, multiple distributed storage system) to prevent unauthorized changes to the event log data, to provide a high level of data integrity and confidentiality.

2.3 Security Assurance

As introduced in **Section 2.1**, security assurance represents the second component of the robustness scheme. Authentication security assurance is the measure of confidence in the ability of an authentication mechanism to appropriately enforce its security policies (i.e., meet its security objectives).

This high-level security assurance requirements are described in the following sections with requirements specified at each level of robustness. They are also described in detail in *Baseline Security Architecture for IT Systems (ITSG-30)* [**Reference 1**].

2.3.1 Level 1

At Level 1, only some confidence in correct operation is required given the low value or sensitivity of the transactions involved and minor threat environment.

2.3.2 Level 2

At Level 2, a low to moderate level of assured security is required in the absence of an available development record.

2.3.3 Level 3

At Level 3, a moderate level of assured security is required in the absence of an available development record.



2.3.4 Level 4

At Level 4, a moderate to high level of assured security in conventional products is required, and where developers or users are prepared to incur additional security-specific engineering costs.



This page intentionally left blank



Table 1. Authentication Solution Design Requirements

Note: The selection of an authentication solution is based on satisfying the requirements from all five of the authentication design requirement categories.

	Design Requirement Categories	Robustness Levels			
		Level 1	Level 2	Level 3	Level 4
Strength of Mechanism	Authentication Factors	At least one factor required.	At least one factor required.	At least two factors required.	At least two factors required.
	Authentication Tokens	<p>At least one of the following tokens required:</p> <p>Something the user knows</p> <ul style="list-style-type: none"> ▪ Password (subject to password rules) ▪ Pre-registered secret token <p>Something the user has</p> <ul style="list-style-type: none"> ▪ Look-up secret token (printed) ▪ Look-up secret token (electronic) ▪ Soft crypto token (with activation data) ▪ Out-of-band secret token ▪ One-time password token ▪ Hardware crypto token (with activation data) <p>Something the user is or does</p> <ul style="list-style-type: none"> ▪ Biometric token 	<p>At least one of the following tokens required:</p> <p>Something the user knows</p> <ul style="list-style-type: none"> ▪ Password (subject to password rules) ▪ Pre-registered secret token <p>Something the user has</p> <ul style="list-style-type: none"> ▪ Look-up secret token (printed) ▪ Look-up secret token (electronic) ▪ Soft crypto token (with activation data) ▪ Out-of-band secret token ▪ One-time password token ▪ Hardware crypto token (with activation data) <p>Something the user is or does</p> <ul style="list-style-type: none"> ▪ Biometric token (to be used only in conjunction with a non-biometric token) 	<p>At least two of the following tokens (based on different factors) required:</p> <p>Something the user knows</p> <ul style="list-style-type: none"> ▪ Password (subject to password rules) ▪ Pre-registered secret token <p>Something the user has</p> <ul style="list-style-type: none"> ▪ Look-up secret token (printed) ▪ Look-up secret token (electronic) ▪ Soft crypto token (with activation data) ▪ Out-of-band secret token ▪ One-time password token ▪ Hardware crypto token (with activation data) <p>Something the user is or does</p> <ul style="list-style-type: none"> ▪ Biometric token (to be used only as activation data for another authentication token) 	<p>The following tokens are required (can be combined with other tokens):</p> <ul style="list-style-type: none"> ▪ Hardware crypto token (with activation data): <ul style="list-style-type: none"> ▪ Password (subject to password rules); or ▪ Biometric token



User Authentication Guidance for IT Systems (ITSG-31)

	Design Requirement Categories	Robustness Levels			
		Level 1	Level 2	Level 3	Level 4
Strength of Mechanism	Threat Mitigation <i>(as applicable to environment)</i>	Mitigation against the following threats: <ul style="list-style-type: none"> On-line password guessing Replay 	Mitigation against the following threats: <ul style="list-style-type: none"> On-line password guessing Replay Eavesdropping Session hijacking 	Mitigation against all described threats: <ul style="list-style-type: none"> On-line password guessing Replay Eavesdropping Session hijacking Verifier impersonation/phishing Man-in-the-middle 	Mitigation against all described threats: <ul style="list-style-type: none"> On-line password guessing Replay Eavesdropping Session hijacking Verifier impersonation/phishing Man-in-the-middle
	Cryptographic Module Validation <i>(if a cryptographic module is used)</i>	No minimum cryptographic module validation requirements.	No minimum cryptographic module validation requirements.	FIPS 140-2 Level 1, augmented with Level 2 for identity-based user authentication. <i>(hardware or software)</i>	FIPS 140-2 Level 2, augmented with Level 3 for physical security. <i>(hardware only)</i>
	Authentication Event Logging	No minimum authentication event logging requirements.	Only the following: <ul style="list-style-type: none"> Recording of User ID, Date/Time, and Result Access-control protection against unauthorized access 	Only the following: <ul style="list-style-type: none"> Recording of User ID, Date/Time, and Result Access-control protection against unauthorized access Tamper-detection mechanism against unauthorized changes (e.g., digital signature) 	Only the following: <ul style="list-style-type: none"> Recording of User ID, Date/Time, and Result Access-control protection against unauthorized access Tamper-detection mechanism against unauthorized changes (e.g., using digital signature) Tamper-prevention mechanism against unauthorized changes (e.g., write-once media, multiple distributed storage system).
Security Assurance		<i>This security assurance level (SAL 1) is applicable where only some confidence in correct operation is required given the low value or sensitivity of the transactions involved and minor threat environment.</i>	<i>This security assurance level (SAL 2) is applicable where a low to moderate level of assured security is required.</i>	<i>This security assurance level (SAL 3) is applicable where a moderate level of assured security is required</i>	<i>This security assurance level (SAL 4) is applicable in those circumstances in which a moderate to high level of assured security in conventional products is required, and where developers or users are prepared to incur additional security-specific engineering costs.</i>



3 References

- [Reference 1]** *Baseline Security Architecture for IT Systems*. Communications Security Establishment Canada (CSEC), Draft.

- [Reference 2]** *Electronic Authentication Guideline (SP 800-63)*. National Institute of Standard and Technology (NIST), April 2006.
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

- [Reference 3]** *Guideline on Authentication – Preliminary Draft*. Treasury Board of Canada Secretariat, November 2008.

- [Reference 4]** *Technical Addendum – User Authentication Guidance for IT Systems*. Communications Security Establishment Canada (CSEC), April 2009.

- [Reference 5]** *CNSS Instruction No. 4009 National Information Assurance (IA) Glossary*. Committee on National Security Systems, June 2006.
http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf