



# **E-Authentication**

## **Interim PIN Credential Assessment Profile**

12/19/2003  
release 1.3.0

### **Executive Summary**

This document is the Credential Assessment Profile for Public Key Infrastructure based credentials. It is part of the Credential Assessment Portfolio as described in the E-Authentication Interim Credential Assessment Framework (CAF). The reader is assumed to be familiar with the CAF. This document contains the specific criteria used to assess Personal Identification Number (PIN) based Credential Services (CSs) for use in the E-Authentication Initiative. This profile does not apply to CSs that use PINs in conjunction with hard tokens or specialized software; it only covers the use of PINs in conjunction with standard browsers for remote authentication. Additional criteria may be specified by other profiles.

### **Release Notes**

*Interim Release*

## Document History

Status	Release	Date	Comment	Audience
Released	1.0.0	07/10/03	First Release	Limited
Interim	1.3.0	12/19/03	Released for customer review with the proposal that it be accepted for publication as 2.0.0: a) 4.1 - removal of redundant criteria summary entries; b) §4.2.1 & §4.3.1 - amendment of refs to 'TSM' to NIST SP 800-63.  AND minor proofing amendments which have changed neither the semantics nor the intentions of the document. NB - this document supersedes 1.1.0, which was overtaken by release of the Nov. 2003 draft of NIST SP 800-63 and withdrawn before release.	Customer

## Editors

Chris Loudon  
Kevin Hawkins  
Richard G. Wilsher  
Dave Silver

David Temoshok  
Judy Spencer  
Steve Timchak  
Von Harrison

Bill Burr  
John Cornell  
Steven Sill

# Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1</b>
<b>2</b>	<b>SCOPE .....</b>	<b>1</b>
<b>3</b>	<b>TERMINOLOGY .....</b>	<b>1</b>
<b>4</b>	<b>CRITERIA .....</b>	<b>2</b>
4.1	SUMMARY .....	2
4.2	ASSURANCE LEVEL 1 .....	2
4.2.1	<i>Token Strength</i> .....	2
4.3	ASSURANCE LEVEL 2 .....	3
4.3.1	<i>Token Strength</i> .....	3

## **1 INTRODUCTION**

This document is part of a suite of documents governing the assessment of credentials for use with the E-Authentication Initiative. Please refer to the Interim Credential Assessment Framework (CAF) for an overview. Additional information can be found at <http://www.cio.gov/eauthentication/>. This profile specifies criteria for Credential Services (CSs) that are based on the use of Personal Identification Numbers (PINs) with conventional browsers for remote authentication.

## **2 SCOPE**

This profile contains requirements to be met by any Credential Service (CS), based on the use of simple Personal Identification Numbers (PIN) that are numeric-only to remotely authenticate using a web browser. There may be other requirements for these systems specified by other profiles.

This profile does not apply to systems where PINs are used in conjunction with physical tokens or specialized software.

Criteria presented in any CAP are cumulative through higher assurance levels. Qualification at any Assurance Level requires validated compliance with all criteria for lower levels of assurance. Assessment at a given Assurance Level also requires validated compliance with multiple profiles; refer to the CAF for more information.

## **3 TERMINOLOGY**

This document relies on terminology and definitions established in the Interim Credential Assessment Framework. The most recent version is available at <http://www.cio.gov/eauthentication/>.

## 4 CRITERIA

### 4.1 Summary

	Level 1	Level 2
<b>Token Strength</b>	<input type="checkbox"/> Basic PIN <input type="checkbox"/> Modifiable	<input type="checkbox"/> Strong PIN

### 4.2 Assurance Level 1

#### 4.2.1 Token Strength

Tag	Description
Basic PIN	Numeric only. The PIN and the controls used to limit on-line guessing attacks shall ensure that an attack targeted against a selected user/PIN shall have a probability of success of less than $2^{-11}$ (1 chance in 2,048) over the life of the PIN. Refer to NIST SP 800-63 Appendix A to calculate resistance to online guessing.
Modifiable	Subscribers must be able to change their PIN.

## 4.3 Assurance Level 2

### 4.3.1 Token Strength

<b>Tag</b>	<b>Description</b>
Strong PIN	The PIN and the controls used to limit on-line guessing attacks shall ensure that an attack targeted against a selected user/PIN shall have a probability of success of less than $2^{-16}$ (1 chance in 65,536) over the life of the PIN. Refer to NIST SP 800-63 Appendix A to calculate resistance to online guessing.