NISTIR 7849

A Methodology for Developing Authentication Assurance Level Taxonomy for Smart Card-based Identity Verification

Ramaswamy Chandramouli

http://dx.doi.org/10.6028/NIST.IR.7849

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 7849

A Methodology for Developing Authentication Assurance Level Taxonomy for Smart Card-based Identity Verification

Ramaswamy Chandramouli
Computer Security Division
Information Technology Laboratory

http://dx.doi.org/10.6028/NIST.IR.7849

March 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency or Internal Report 7849
40 pages (March 2014)

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

Smart cards (smart identity tokens) are now being extensively deployed for identity verification for controlling access to Information Technology (IT) resources as well as physical resources. Depending upon the sensitivity of the resources and the risk of wrong identification, different authentication use cases are being deployed. Assignment of authentication strength for each of the use cases is often based on: (a) the total number of three common orthogonal authentication factors – What You Know, What You Have and What You are, and (b) the entropy associated with each factor chosen. The objective of this paper is to analyze the limitation of this approach and present a methodology for assigning authentication strengths based on the strength of pair wise bindings between the five entities involved in smart card based authentications – the card (token), the token secret, the card holder, the card issuer, and the person identifier stored in the card. The rationale for the methodology is based on the following three observations: (a) The form factor of the smart identity token introduces some threats of misuse; (b) the common set of credentials objects provisioned to a smart card embody bindings to address those threats and (c) the strength of an authentication use case should therefore be based on the number and type of binding verifications that are performed in the constituent authentication mechanisms.The use of the methodology for developing an authentication assurance level taxonomy for two real world smart identity token deployments is also illustrated.

Keywords

card issuer; cardholder trait (biometric); person identifier; smart identity token; token secret.

Acknowledgements

The author, Ramaswamy Chandramouli (Mouli), would like to thank his colleagues Hildegard Ferraiolo and Patrick Grother for serving as reviewers for this document. The author also acknowledges Elizabeth Lennon for her technical editing and administrative support.

Audience

This document analyzes the authentication mechanisms used with smart identity tokens based on some fundamental principles in order to derive a metric for assigning appropriate authentication strengths to them. The potential audiences that could benefit from this document are:

- Public and Private Sector communities seeking to deploy smart cards for identity verification (smart identity tokens) for various access control applications;
- Vendor communities seeking to personalize smart identity tokens; and
- Testing communities seeking to evaluate smart identity token deployments for required authentication strengths.

TABLE OF CONTENTS

1. Introduction

With the proliferation of web-based applications and e-commerce transactions, the field of identity verification or authentication of humans has evolved from the concept of using identities tied to a specific entitlement (e.g., a driver's license or passport) to the concept of using generic trusted digital identities that can be relied upon and consumed by multiple types of service providers. Another evolutionary trend is the use of multiple form factors to carry or support these trusted identities. Smart cards and Smart phones are two such form factors.

Smart cards are now being extensively deployed for identity verification for controlling access to Information Technology (IT) resources as well as physical resources [Ham2001, Kum2008, TWIC2008].We refer to those types of cards as Smart Identity Tokens and use the two terms interchangeably throughout this paper. These types of smart cards generally carry: (a) A Person Identifier (PI), (b) A Secret (TS) usually in the form of a cryptographic key [EAG2013], (c) A Credential linking the Secret and the Identifier (CR) and (d) A Credential linking the Identifier with a Personal Trait of the Cardholder (e.g., biometric) (BR). Along with these data, another secret, a PIN (a combination of numbers) is often used for: (a) Activating the card (token) and for (b) Restricting access to certain data objects and operations. In some instances, presentation of a live biometric data (such as a fingerprint) is used to enable the above functions instead of a PIN. In any enterprise deploying smart cards, there may be different types of resources that may have to be protected by restricting access to only those whose identity is verified through a smart card based authentication mechanism. Depending upon the sensitivity of the resource and the risk associated with wrong identification of the entity requesting access to those resources, authentication mechanisms use different combinations of the four data types enumerated above (i.e., PI, TS, CR or BR) along with/without an activation data. One or more of authentication mechanisms in turn constitute an authentication use case and a typical identification verification deployment instance uses multiple authentication use cases to cover access to resources of multiple sensitivity levels.

The choice of an authentication use case (irrespective of whether a smart identity token is used or not) in any deployment instance, therefore, depends upon the overall authentication assurance level provided by the combination of constituent authentication mechanisms.The usage of a token by a claimant during an authentication event results in a value called Authenticator that is generated by the token and is transmitted from the token to the authentication module or the verifier. The basis for designating an authentication strength associated with a token is a fundamental unit called "Authentication Factor". There are three main authentication factors [OMB2003]:

- What the Entity Knows (e.g., Password, PIN, etc)
- What the Entity Has (e.g., possession of a token that generates one-time passwords)
- What the Entity Is (e.g., inherent physiological characteristic such as a fingerprint)

A token that uses one of the above three factors is called a single factor token (e.g., a password that belongs to "What the Entity Knows" factor). A token that uses a combination of two or more of the above factors is called a multi-factor token. A smart card that contains an embedded private cryptographic key (thus using "What the Entity Has" authentication factor) that can be used to generate an authenticator when it is activated by a PIN, (using the "What the Entity Knows" authentication factor) is deemed a two-factor token. An authentication use case may use one or more tokens and hence may involve the use of one or more authentication factors. In general, the authentication strength associated with an authentication use case is determined based on the combination of the following metrics:

- The number of authentication factors used in the authentication use case
- The Entropy associated with each of the authenticator factors used

In this publication, we argue that the logic for assigning authentication strength based on the number of authentication factors in an authentication use case is valid only under certain limiting conditions and that these conditions do not hold in the case of authentication use cases using smart cards as identity tokens. This is the rationale for proposing a new methodology for: (a) Assigning authentication strengths or levels for various authentication use cases involving smart identity tokens and (b) Deriving an authentication assurance taxonomy using the relative strengths of all authentication use cases specified for the deployment.

The limitations of the authentication factor-based approach for determining authentication assurance level and justifications for a new methodology are outlined in Sec. 2. The overall anatomy of smart card-based identity verification is analyzed in Sec. 3. The analysis leads to the identification of bindings established in the initial phases of smart card-based identity verification deployment which then forms the foundational concept for our methodology. The next two sections (Sec. 4 and 5) describe the core steps of our methodology. In Sec. 4, we enumerate the typical set of data objects found in smart cards used in identity verification, the trust bindings each of those objects embodies and the primitive authentication mechanisms that verify those bindings. Section 5 goes on to demonstrate the process of deriving an authentication strength (based on the composition of verified bindings as well as their number and type) for any authentication use case constructed using the primitive authentication mechanisms discussed in Sec. 4. By examining the composition of the "set of verified bindings" in various authentication use cases, it is possible to derive partial orderings among those use cases. These partial orderings, in turn, are used to develop the authentication assurance taxonomy for the total set of authentication use cases specified for a smart identity token deployment. Section 6 provides the conclusions and benefits of our methodology.

In Appendices A and B we demonstrate the use of our methodology to real-world smart identity token deployments. The deployments are: (a) Personal Identity Verification (PIV) program of the US Government and (b) Transporation Worker Identification program (TWIC) of the Department of Homeland Security. More specifically, Appendix A describes the application of our methodology to PIV authentication use cases while Appendix B illustrates our methodology for TWIC authentication use cases. The outcome of the assignment of authentication assurance levels based on our methodology to the complete set of authentication use cases in these two deployments results in an authentication assurance taxonomy for each of them.

2. Limitations of Authentication Factor-Based Approach

In identity verification schemes where trusted identities are provisioned to devices with various form factors (e.g., smart cards, smart phones etc), the authentication factor-based approach for determining authentication strengths (for authentication mechanisms) does not provide the right measure of identity assurance. This is due to the fact that the form factor of the devices introduces some threats of misuse which may not be adequately detected by some authentication mechanisms used in those devices-based identity verification deployments. These threats are briefly described here below. We use the abbreviation convention FF-Tx to designate each threat (FF stands for Form Factor and Tx is the sequence number for the threat)

- FF-T1: STOLEN DEVICE (with unaltered credentials): The person trying to obtain authentication using the device is not the owner of the device/legitimate holder of the credential. This results in "Impersonation" threat.
- FF-T2: CLONED DEVICE (with unaltered credentials): The device containing the credential could be a clone of the device where the original credentials had been provisioned by the legitimate identity provider/credential issuer/authorized device issuer. The threat here is "Unauthorized Proliferation of Credentials and Resulting Misuse."
- FF-T3: FORGED CREDENTIAL: The credential on the device has not originated from an authorized issuer/identity provider. Specifically it does not carry the proof that it was created/assigned by an authorized identity provider and has not been tampered with after issuance.

Thus we see that there is a need for an authentication assurance methodology that takes into account inherent characteristics of the device supporting the trusted identities. Since smart card is the most prevalent device used for provisioning of credentials, we now proceed to analyze the anatomy of smart card-based identity verification in the next section.

3. Anatomy of Smart Card-Based Identity Verification

Smart card-based identity verification is the most widely deployed form of device-based authentication scheme where trusted identities are provisioned to credit card-sized plastic cards embedded with an Integrated Circuit Chip (ICC). A deployment instance may use multiple authentication use cases depending upon the sensititivity of the various resources that are sought to be protected in its environment. An authentication use case in turn will consist of one or more authentication mechanisms. Every authentication mechanism, in this context, will involve use of the device (the smart card or smart identity token[1] in our context) but some of them may not require participation of the user/bearer of the device since the underlying protocol may not call for the bearer input (e.g., a PIN or biometric sample).

In order to assess the authentication strengths associated with authentication mechanisms using a smart card, we need to look at the typical phases involved in any smart card-based identity verification scheme (smart identity token) deployment. They are:

- Identity Token Eligibility Determination Phase
- Identity Token Issuance Phase
- Identity Token Usage Phase

Out of the three phases above, the authentication mechanisms and by extension the authentication use cases come into the picture only in the Identity Token Usage Phase. Since the objective of this paper is a methodology for assignment of authentication assurance level/strength for authentication use cases, our focus should be on the Identity Token Usage phase. However, we find that in order to arrive at a meaningful authentication strength metric, we need to examine all three phases because of the following rationale.

- The overall authentication strength in authentication use cases deployed in the Identity Token Usage phase is derived from the combination of trust levels in its constitutent authentication mechanisms. The trust level of an authentication mechanism, in turn, is based on the number of trust bindings (embedded in credential objects) it verifies.

- The trust in the set of credential objects that are provisioned to the smart identity token during the Identity Token Issuance phase comes from the bindings it embodies and from the overall security of the system processes used in their generation – security for the data repositories holding the enrollment records, trust in attestion authority that is vouching for credential bindings (e.g., Certificate Authorities (CAs) for digital certificates).

- The basis for creation of credential objects in turn is the “Proofed Identity” which is embodied in the set of data records called enrollment records that are created after a successful “Identity Proofing” process in the Identity Token Eligibility Determination phase.

Thus we see that the trust marker or “Proofed Identity” for the individual being authenticated is established in the Token Eligibility Determination Phase which together with other data in the enrollment records forms the basis for creation of credential objects in the Token Issuance phase. The credential objects by definition embody a “stamp of authority” or trust binding in each of them. Since the purpose of any authentication mechanism is to

[1] We will the two terms interchangeably in this document

verify/validate those bindings, any assessment of its strength should involve the set of bindings it verifies as a prime metric. *Hence identification of the verified bindings of an authentication mechanism logically forms the first step of our methodology*. Before we proceed to that step, we take a look at the various activities leading up to the creation of those credential objects and the issuance of the smart identity token in order to fully understand the nature of the trust chain.

3.1 Trust Creation in Identity Token Eligibility Determination Phase

The primary processes in this phase are identity proofing and enrollment/registration. The “identity proofing” starts with verification of one or more source documents attesting to the identity of the intended card/credential holder together with/without consultation of authoritative data repositories (e.g., use of credit history records and the use of Criminal History database for background verification). The degree of trust in the identity of the individual undergoing identity proofing process is determined by the nature and number of source documents used. This trust is then concretized in an artifact called "proofed identity" in order to be carried over to the next phase of the smart identity token deployment. The most common artifact is usually a set of fingerprints [NSTC2008] which are collected at the conclusion of a successful identity proofing process. This artifact thus creates the “binding” between the person who has undergone identity proofing and the "prospective credential holder/identity token holder" since the tokens are going to carry the provisioned credentials.The biographical details gathered from the source documents together with the proofed identity are stored in a formal system of records (called the enrollment records) during the enrollment/registration process of this phase.

3.2 Creation of Trust Bindings in the Identity Token Issuance Phase

The processes in this phase include the following:

- Assignment of a unique person identifier to the token holder: The person identifier can either be: (a) locally unique (e.g., employee number in an organization) or (b) globally unique (i.e., UUID).

- Creation of credentials that embody various types of “trust bindings” and provisioning them to the token/smart card: The choice of a trust binding and by extension the choice of a credential that embodies that binding is based on the degree of assurance it provides against exploitation of threats EF-T1, EF-T2 and EF-T3 described in section 2. The required assurance, at the minimum, are:

  (a) The assigned person identifier has originated from an authorized credential/token issuer (assurance against the threat of faked or forged credential –FF-T3);

  (b) The assigned person identifier pertains to the person who has been successfully “identity proofed”.It is for this purpose that the “proofed identity” created in the token eligibility determination phase is used (assurance that the token recipient is the person who has undergone “identity proofing”);

  (c) The token instance carrying the person identifier is the physical copy to which the identifier was provisioned by the authorized token issuer (assurance against the threat of cloned token-FF-T2); and

  (d) The person presenting the token (token holder or cardholder) is the person to whom the token was issued by the authorized token issuer. (assurance against the threat of stolen card/impersonation –FF-T1).

- The physical handover of the smart identity token to the legitimate credential owner: Here we need the trust (or assurance) that the person receiving the physical token is the same person for whom identity proofing was done and whose credentials are now provisioned to the token. This assurance is obtained by making the token recipient authenticate against the proofed identity created during the token eligibility phase and now provisioned to the token. For example if a set of fingerprints collected during enrollment is