Authentication Assurance Level Taxonomies for Smart Identity Token Deployments - A New Approach

Ramaswamy Chandramouli

Authentication Assurance Level Taxonomies for Smart Identity Token Deployments - A New Approach

Ramaswamy Chandramouli

National Institute of Standards and Technology Gaithersburg, MD, USA
mouli@nist.gov

Abstract. Authentication assurance level taxonomies that have been specified in many real-world smart identity token deployments do not fully reflect all the security properties associated with their underlying authentication mechanisms. In this paper we describe the development and application of a new methodology called SID-AAM (where the abbreviation stands for Smart Identity Token - Authentication Assurance Level Methodology) that identifies a new set of authentication factors appropriate for this technology, identifies all the security properties that need to be verified based on bindings between various entities involved in the authentication processes and then derives an authentication assurance level taxonomy based on the set of security properties verified in the various authentication modes specified in the deployment. The advantages of SID-AAM methodology compared to current approaches for determining authentication assurance levels for smart identity token deployments are highlighted.

1 Introduction

Smart Cards as identity tokens (or Smart Identity Tokens) are being increasingly deployed in the government and private sector. An authentication mode as specified in smart identity token deployments, consist of one or more authentication mechanisms. An authentication mechanism generally is classified as belonging to one of the following three types (also called Authentication Factors): (a) What you Know (b) What you Have and (c) What you Are. The authentication assurance level for an authentication mode is determined using a combination of the authentication factor coverage (one, two or three) and the strength of individual mechanism constituting that mode. In authentication processes involving smart identity tokens, the artifact that provides the "What you Have" factor can be stolen and hence a new methodology to analyze the authentication modes associated with Smart Identity Token deployments is needed and that is the main focus of this paper. The organization of the rest of the paper is as follows: In Section 2, we take a close look at the functionality of smart identity tokens and derive a new set of authentication factors that is appropriate for authentication processes enabled by that functionality. Section 3 describe the development of

our methodology for analyzing the strength of individual authentication modes (and hence designating an authentication assurance level) and by extension an authentication assurance level taxonomy for the entire smart identity token deployment, and is the main contribution of this paper. We use the acronym SID-AAM to refer to this methodology where the abbreviation stands for Smart Identity Token - Authentication Assurance Methodology. In Section 4, we outline the advantages of our methodology as compared to approaches based on traditional authentication factors for deriving authentication assurance levels.

2 Smart Identity Tokens - Functionality and Applicable Authentication Factors

In the context of this paper, a smart identity token is a plastic card with an ICC (integrated circuit chip) often called a smart card that has the capability to: (a) store a large identifier (SID-F1) (b) store other attributes associated with unique identifier (SID-F2) (c) store a tamper-proof cryptographic secret (SID-F3) and (d) control release of token secret through a secret shared between the token and holder (SID-F4). Based on these capabilities we find that authentication factors appropriate for smart token based authentication (we will them as SID authentication factors) are: (a) Authentication using credentials (SID-AF1) (b) Authentication using cryptographic secret (SID-AF2) and (c) Authentication using a digitally bound combination of credentials and cryptographic secret with or without user control of the secret (SID-AF4). Hence an authentication mode specified in a smart token deployment consists of one or more authentication mechanisms each based on one of the authentication factors listed above.

3 Methodology for Determining Authentication Assurance Level Taxonomies for Smart Identity Token Deployments (SID-AAM)

Next our goal is to develop a methodology by which any deployment authentication mode can be assigned an authentication assurance level and by extension an authentication assurance level taxonomy for the entire deployment scenario. To get to this goal we formulate the following strategic objectives: (a) identify a set of primitive authentication modes for smart identity tokens (called SID primitive authentication modes) and associate a set of security properties associated with each mode. Identify some partial orders among SID primitive authentication modes based on security property containment (b) Express any deployment authentication mode in terms of SID primitive authentication mode (c) Based on property aggregation (adding up all security properties satisfied by all SID primitive authentication modes within a deployment authentication mode) and partial orders among primitive authentication modes themselves, derive an authentication assurance level for a deployment authentication mode and (d) The assurance levels associated with all deployment authentication modes

used in a particular deployment then provides the authentication assurance level taxonomy for that smart identity token deployment.

To realize our strategic objectives, our SID-AAM methodology adopts the following concrete steps. (a) SID-AAM - Step 1: View the entire spectrum of activities in a smart identity token deployment as consisting of two distinct phases - the token issuance phase and token usage phase. Perform a detailed review of all activities/sub tasks in the token issuance phase and derive the set of security properties introduced by each of the activities. (b) SID-AAM-Step 2: Using the set of SID authentication factors for smart identity tokens (derived in section 2) and the technology of smart token usage, derive a set of SID primitive authentication modes. (c) SID-AAM-Step 3: Identify the set of generic threats to SID entities. Also identify the set of security properties (that were introduced in the token issuance phase) that are verified by each of the SID primitive authentication modes and the adverse usage scenario that may result under each mode due to realization of those threats and (d) SID-AAM Step 4: Based on the set of verified properties associated with each SID primitive authentication mode, identify partial orders (dominance relationships) among the SID primitive authentication modes. Using these partial orders, derive the authentication assurance level for each of the SID primitive authentication mode. These levels can then be used for deriving an authentication assurance level taxonomy for any SID deployment based on the set of chosen authentication modes in that deployment.

3.1 Derivation of Security Properties introduced in the Token Issuance Phase (SID-AAM Step 1)

The set of activities involved in a smart identity token deployment scenario can broadly be divided into two phases: (a) Token Issuance Phase and (b) Token Usage Phase. The list of token issuance activities are: (a) SID-I1: Identify Population & Eligibility - Target users eligible to receive tokens (b) SID-I2: Creating Credential Repository & Loading the Application on the token (c) SID-I3: Loading Credentials into the Token (d) SID-I4: Generating the token secret and digitally signing the token-secret related data (e) SID-I5: Populating Token Holder Data in Authentication Points and (f) SID-I6: Issue Token to the Legitimate Holder. These activities involve the following entities: (a) SID-E1: Credential Database (ECDB) - an electronic entity (b) SID-E2: Valid Credentials - Authentication Database (AUDB) at Authentication Points - an electronic entity (c) SID-E3: Token Issuer - (For the purpose of security property we treat this as the IT system that personalizes the token) - an electronic entity (d) SID-E4: The Valid Token -physical token issued to the legitimate user - a physical entity (e) SID-E5: The Token Credential - credentials on the token - an electronic entity (f) SID-E6: The Token Secret - an electronic entity and (g) SID-E7: The Token Holder - the legitimate user to whom the token is issued - a human entity. The token issuance activities introduce certain security properties in the form of bindings involving the entities and these security properties are the ones

that have to be verified during the token usage phase. In the context of bindings, we treat the entities Token Secret (SID-E6) and Valid Token (SID-E4) as one entity since to obtain the token secret from the token without destroying the latter requires costly and sophisticated techniques. The list of security properties along with activities that introduces these properties and the participating entities are: (a) SID-AP1: Token Credential- Valid Credential Binding (SID-I5 involving SID-E5 & SID-E2) (b) SID-AP2: Token Credential-Token Issuer Binding (SID-I3 involving SID-E5 & SID-E3) (c) SID-AP3: Token Secret (Valid Token)-Token Issuer Binding (SID-I4 involving SID-E6/E4 & SID-E3) (d) SID-AP4: Token Secret (Valid Token)-Token Issuer-Token Holder Binding (Additional implementation feature under SID-I4 that enables user control of token secret and thus involves SID-E6/E4, SID-E3 & SID-E7)) (e) SID-AP5: Token Secret (Valid Token)-Token Issuer-Token Credential Binding (Another implementation feature under SID-I4 that digitally binds token secret and token credential and thus involves SID-E6/E4, SID-E3 & SID-E5) and (f) SID-AP6: Token Secret (Valid Token) - Token Issuer - Token Credential - Token Holder Binding (Another implementation feature under SID-I4 that digitally binds token secret and token credential as well as enables user control of token secret and thus involves SID-E6/E4, SID-E3, SID-E5 & SID-E7)

3.2 Deriving SID Primitive Authentication Modes (SID-AAM Step 2)

Each of the SID authentication factors for smart identity tokens (derived in Section 2) may have different implementations with different strengths and each implementation then becomes a SID primitive authentication mode. The list of SID primitive authentication modes are: (a) PAM-CR1: Verify that the credentials on the token are valid (SID-AF1) (b) PAM-CR2: Verify that the credentials on the token are Valid and Authentic (SID-AF1) (c) PAM-TS1: Verify that the token has a valid, authentic Secret (SID-AF2) (d) PAM-TS2: Verify that the token has a valid, authentic Secret and the user has control over the secret (SID-AF2) (e) PAM-CR-TS1: Verify that there is a digital binding of the Valid, Authentic Token Credential and a Valid, Authentic Token Secret (SID-AF3) and (f) PAM-CR-TS2: Verify that there is a digital binding of the Valid, Authentic Token Credential and a Valid, Authentic Token Secret and the user has control over the secret (SID-AF3. Now we that we have the set of security properties introduced in token issuance phase (from SID-AAM Step1) and the set of SID primitive authentication modes (from SID-AAM Step 2), our next task is to analyze the security property or properties that each SID primitive authentication mode verifies and the potential adverse usage scenarios that may affect the integrity of that property verification capability. To derive the latter, we need to look at the threats to SID entities. These threats along with the affected SID entities are: (a) SID-T1: A valid issued token (SID-E4) along with its embedded secret (SID-E6) may be easily stolen because of the small form factor of the artifact (b) SID-T2: The Token Credential (SID-E5) (along with its associated Digital Signature) may be duplicated on a cloned/illegal token and (c)

SID-T3: The Token Credential (SID-E5) may be altered/tampered on a valid issued token.

3.3 Security Properties Verified /Adverse Usage Scenario in Various SID Primitive Authentication Modes (SID-AMM Step 3)

We now proceed to analyze the security strength of each of the SID primitive authentication modes (under each of the SID authentication factors) in terms of the set of verified security properties as well as potential adverse usage scenario associated with its deployment. (a) PAM-CR1: Verify that the credentials on the token are valid with Token Credential - Valid Credential Binding (SID-AP1) as property verified with the Claimant with legitimate, stolen token with Valid Credentials (OR) Claimant with Cloned token with Valid Credentials as the potential adverse scenario. (b) PAM-CR2: Verify that the credentials on the token are Valid and Authentic Token Credential - Valid Credential Binding (SID-AP1) & Token Credential - Token Issuer Binding (SID-AP2) as verified properties with the Claimant with legitimate, stolen token with Valid, Authentic Credentials (OR) Claimant with Cloned token with Valid, Authentic Credentials as potential adverse scenario (c) PAM-TS1: Verify that the token has a valid, authentic Secret with Token Credential - Valid Credential Binding (SID-AP1) & Token Secret (Valid Token) - Token Issuer Binding (SID-AP3) as verified properties with Claimant with a legitimate, stolen token with or without tampered Credentials as potential adverse scenario. (d) PAM-TS2: Verify that the token has a valid, authentic Secret and the user has control over the secret with Token Credential - Valid Credential Binding (SID-AP1), Token Secret (Valid Token) - Token Issuer Binding (SID-AP3) & Token Secret (Valid Token)-Token Issuer-Token Holder Binding (SID-AP4) as verified properties with Claimant with a legitimate, owner-possessed token with tampered credentials as potential adverse usage scenario. (e) PAM-CR-TS1: Verify that there is a digital binding of the Valid, Authentic Token Credential and a Valid, Authentic Token Secret with Token Credential - Valid Credential Binding (SID-AP1), Token Credential - Token Issuer Binding (SID-AP2), Token Secret (Valid Token) - Token Issuer Binding (SID-AP3) & Token Secret (Valid Token) - Token Issuer - Token Credential Binding (SID-AP5) as verified properties with the Claimant with a legitimate, stolen token with Valid, Authentic Credentials as potential adverse scenario. (f) PAM-CR-TS2: Verify that there is a digital binding of the Valid, Authentic Token Credential and a Valid, Authentic Token Secret and the user has control over the secret with Token Credential - Valid Credential Binding (SID-AP1), Token Credential - Token Issuer Binding (SID-AP2) & Token Secret (Valid Token) - Token Issuer Binding (SID-AP3), Token Secret (Valid Token) - Token Issuer-Token Holder Binding (SID-AP4), Token Secret (Valid Token) - Token Issuer - Token Credential Binding (SID-AP5) & Token Secret (Valid Token) - Token Issuer - Token Credential - Token Holder Binding (SID-AP6) with no potential adverse usage scenario.

3.4 Deriving Authentication Assurance Level Taxonomy for SID-based Authentications (SID-AAM Step 4)

Now that we have a set of verified security properties associated with each SID primitive authentication mode, our logic for deriving an authentication assurance level for each of these modes and by extension an authentication assurance level taxonomy for a smart identity token deployment should be based on property containment relationships between any pair of SID primitive authentication modes. Let us a choose a hierarchical chain of levels with number suffixes denoting the place in the chain - levels L0, L1, L2, L3 etc with L0 denoting the lowest level in the chain. By looking at the set of security properties verified by each SID primitive authentication mode in Section 3.1, 3.2 and 3.3, we arrive at the following dominance relationships. First we will look at dominance relationship between any two modes within a SID authentication factor and then look at such relationships between modes across authentication factors. The list of dominance relationships of the first category is as follows:

$$\text{PAM-CR2} > \text{PAM-CR1(within SID-AF1 factor)} \tag{1}$$

$$\text{PAM-TS2} > \text{PAM-TS1 (within SID-AF2 factor)} \tag{2}$$

$$\text{PAM-CR-TS2} > \text{PAM-CR-TS1 (within SID-AF3 factor)} \tag{3}$$

The list of dominance relationships between SID primitive authentication modes across SID authentication factors are as follows:

$$\text{PAM-TS1} > \text{PAM-CR1} \tag{4}$$

$$\text{PAM-CR-TS1} > \text{PAM-CR1} \tag{5}$$

$$\text{PAM-CR-TS1} > \text{PAM-CR2} \tag{6}$$

$$\text{PAM-CR-TS1} > \text{PAM-TS1} \tag{7}$$

$$\text{PAM-CR-TS2} > \text{PAM-CR1} \tag{8}$$

$$\text{PAM-CR-TS2} > \text{PAM-CR2} \tag{9}$$

$$\text{PAM-CR-TS2} > \text{PAM-TS1} \tag{10}$$

$$\text{PAM-CR-TS2} > \text{PAM-TS2} \tag{11}$$

By looking at the dominance relationships, we find that every SID primitive authentication mode dominates PAM-CR1 and that no mode dominates PAM-CR-TS2. Hence we can assign the lowest and highest authentication assurance levels respectively to these two modes. Let us start with assigning L0 to PAM-CR1 and look for assigning levels from the hierarchy. Using relationship 1 we can assign level L1 to PAM-CR2. By using relationship 4 and the fact that PAM-CR2 and PAM-TS1 do not have any dominant relationships between them, we can both assign them to level L2. By using this logic we arrive at the following authentication assurance levels for all SID primitive authentication modes as follows: Level L0: Qualifying SID primitive authentication mode: PAM-CR1 Level L1: Dominates PAM-CR1. Qualifying modes: PAM-CR2 and PAM-TS1 Level L2: Dominates any mode in Level L1 or involves more SID authentication

factors but no mutual dominance relationship. Qualifying modes: PAM-TS2 and PAM-CR-TS1 Level L3: Dominates all modes. Qualifying mode: PAM-CR-TS2

4 Advantages of SID-AAM Methodology

Published Literature for analyzing authentication assurance levels for smart identity token-based authentication processes concentrate either on strength of authentication protocols [1, 2] or coverage of conventional authentication factors [3, 4]. As far as we know SID-AAM is the only methodology that determines authentication assurance levels based on the set of security properties verified. The characteristics that makes this methodology robust are: (a) takes into account all technology-specific entities participating in the authentication processes (b) formulates a set of authentication factors that is specific to SID technology and (c) is based on verified security properties that involve binding between entities as well as consideration of the threats that can affect the integrity of these verifications.

References

1. Securing e-business applications using Smart Cards, IBM Systems Journal, Vol 40, Number 3, 2001, http://www.research.ibm.com/journal/sj/403/hamann.html
2. Kumar, M.: New Remote User Authentication Scheme Using Smart Cards, IEEE Transactions on Consumer Electronics. Volume 50, Issue 2, 597 - 600 (2004)
3. FIPS 201 - Personal Identity Verification of Federal Employees and Contractors, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
4. TWIC Reader Hardware And Card Application Specification, May 30, 2008, http://www.tsa.gov/assets/pdf/twic_reader_card_app_spec.pdf