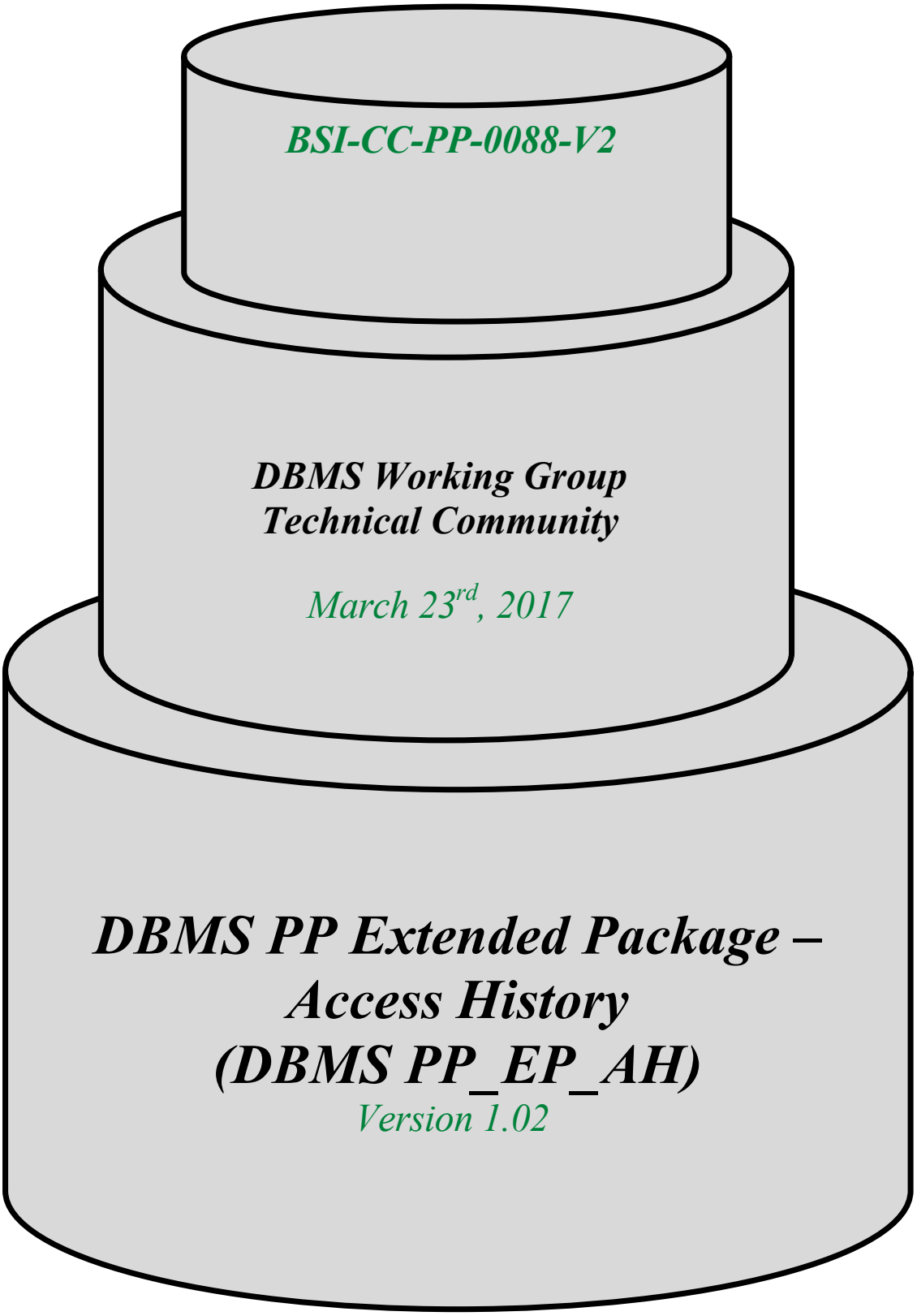
BSI-CC-PP-0088-V2
DBMS Working Group
Technical Community
March 23rd, 2017
DBMS PP Extended Package –
Access History
(DBMS PP_EP_AH)
Version 1.02

Revision History

Version	Date	Description
1.0	November xx, 2016	Instantiation of the Extended Package
1.01	January 30th, 2017	Removal of "draft" watermark. Addition of T.IA.MASQUERADE rationale as supportive of reducing O.ACCESS_HISTORY in table 3.
1.02	March 23rd, 2017	Minor corrections after validator's review.

Further information, including the status and updates of this extended package can be found in the DBMS WG/TC project area on the CCUF website:
https://ccusersforum.onlyoffice.com/products/projects/tasks.aspx?prjID=410822

Comments on this document should be submitted to the DBMS WG/TC workspace. The comment should include the title and version of the document, the page, the section number, the line number, and the detailed comment and recommendation.

Protection Profile Title:

DBMS PP Extended Package – Access History

Common Criteria Version:

This Extended Package was updated using Version 3.1 of the Common Criteria (CC) [REF 1].

Table of Contents

List of Tables

1 INTRODUCTION TO THE DBMS PP EXTENDED PACKAGE

1.1 DBMS PP Extended Package Identification

Title: DBMS PP Extended Package – Access History

DBMS PP Extended Package Abbreviation: AH

Sponsor: DBMS Working Group / Technical Community

CC Version: Common Criteria (CC) Version 3.1 R4

EP Version: 1.02

Publication Date: 23rd March, 2017

Keywords: database management system, DBMS PP, DBMS, COTS, access history

1.2 DBMS PP Extended Package Overview

The base DBMS PP Security Problem Definition does not include a security objective relating to access history.

While many organizations do not specify this objective as part of their security problem definition, this additional security objective may need to be included in the security problem definition by some organizations in order to support further mitigation of the threats of T.ACCESS_TSFDATA, T.IA_MASQUERADE and T.TSF_COMPROMISE. This is achieved by allowing trained users to review their access history in order to help identify unauthorized access attempts.

This extended package supplements the DBMS PP by adding the TOE Security Objective O.ACCESS-HISTORY and the security functional requirement supporting that objective.

1.3 DBMS PP Extended Package Framework

The DBMS PP Extended Package – Access History is part of the Database Management System Protection Profile framework defined in [DBMS PP] chapter 1.3. An ST author may optionally use this document specifying an extended package in addition to the DBMS base protection profile defined with [DBMS PP] chapters 3ff.

1.4 Structure of the Extended Package

This document is structured as follows:

- Chapter 1 provides the introduction into the DBMS PP extended package.
- Chapter 2 specifies the conformance claims for the DBMS PP extended package.
- Chapter 3 contains the security problem definition applicable to this DBMS PP extended package.

- Chapter 4 defines the objectives to be covered by TOEs that are conformant to this DBMS PP extended package.
- Chapter 5 contains the definition of extended components used in this DBMS PP extended package.
- Chapter 6 holds the security requirements definition for this DBMS PP extended package. database management system.

1.5 References

The references given in the [DBMS PP] are also applicable to this document. The following references are also applicable to this document:

DBMS PP Protection Profile for Database Management Systems (Base Package) V 2.12

1.6 Document Conventions

The document convention explained in Chapter 1.4 of [DBMS PP] are applicable in this document.

2 CONFORMANCE CLAIMS

The following sections describe the conformance claims of the Database Management System Protection Profile (DBMS PP).

2.1 Conformance with CC

This extended package does not augment the conformance claim of the DBMS PP base specified in [DBMS PP] chapter 3.

2.2 Extended Package Conformance Rules

This extended package does not depend on other DBMS PP extended packages.

This package can only be claimed together with the DBMS PP base package, in the version defined in [DBMS PP].

This extended package does not conflict with any other DBMS PP extended package at the time of publication.

3 SECURITY PROBLEM DEFINITION

The security problem definition of the DBMS PP Extended Package – Access History does not change the security problem definition of the DBMS PP base.

3.1 Threats

This extended package neither adds to nor alters the threats given in [DBMS PP].

3.2 Organizational Security Policies

This extended package neither adds to nor alters any organizational security policies given in [DBMS PP].

3.3 Assumptions

This extended package neither adds to nor alters the assumptions given in [DBMS PP].

4 SECURITY OBJECTIVES

This section identifies the additional security objectives of the TOE and its supporting environment met by this extended package.

These security objectives identify the responsibilities of the TOE and its environment in meeting the security problem definition (SPD).

4.1 TOE Security Objectives

This extended package specifies one additional security objective in addition to those given in [DBMS PP].

Table 1: Additional TOE Security Objectives

Objective Name	Objective Definition
O.ACCESS_HISTORY	The TOE will store information related to previous attempts to establish a session and make that information available to the user.

4.2 Operational Environment Security Objectives

This extended package neither adds to nor alters the operational environment security objectives given in [DBMS PP].

4.3 Rationale for Security Objectives

The table below gives a summary of the policies, and threats relating to the TOE security objectives.

Security objectives coverage

Table 2: Coverage of Security Objectives for the TOE

Objective Name	SPD coverage
O.ACCESS_HISTORY	T.TSF_COMPROMISE (from DBMS PP base) T.ACCESS_TSFDATA (from DBMS PP base) T.IA_MASQUERADE (from DBMS PP base)

Rationale for the Security objectives sufficiency

The table below gives the rationale for the TOE security objectives. In this extended package security objective O.ACCESS_HISTORY is supportive in reducing the threats T.ACCESS_TSFDATA, T.IA_MASQUERADE and T.TSF_COMPROMISE given in the base DBMS PP.

Table 3: Additional rationale for TOE security objectives sufficiency

Threat/Policy	TOE Security Objectives Addressing the Threat/Policy	Rationale
T.ACCESS_TSFDATA A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.	O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will store the information that is needed to advise the user of previous authentication attempts and allows this information to be retrieved.
T.IA_MASQUERADE A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.	O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	O.ACCESS_HISTORY requiring logging of unsuccessful attempts to authenticate with the TOE, which might be an indicator for masquerading attempts, would be supportive in further diminishing the threat
T.TSF_COMPROMISE A user or a process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.	O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will be able to store and retrieve the information that will advise the user of the last successful login attempt and performed actions without his/her knowledge.

5 EXTENDED SECURITY FUNCTIONAL REQUIREMENTS

This extended package defines one extended SFR.

5.1 Extended Security Functional Requirements Specified By This Extended Package

FTA_TAH_(EXT).1 TOE access information

FTA_TAH_(EXT).1 TOE access information provides the requirement for a TOE to make available information related to attempts to establish a session.

Component levelling

FTA_TAH_(EXT).1 is not hierarchical to any other components.

Management: FTA_TAH_(EXT).1

There are no management activities foreseen.

Audit: FTA_TAH_(EXT).1

There are no auditable events foreseen.

FTA_TAH_(EXT).1 TOE access information

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAH_(EXT).1.1

Upon a session establishment attempt, the TSF shall store

a. the [date and time] of the session establishment attempt of the user.

b. the incremental count of successive unsuccessful session establishment attempt(s).

FTA_TAH_(EXT).1.2

Upon successful session establishment, the TSF shall allow the [date and time] of

a. the previous last successful session establishment, and

b. the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the previous last successful session establishment

to be retrieved by the user.

5.2 Rationale For The Extended Security Functional Requirement

The table below presents a rationale for the inclusion of the extended functional security requirements found in this extended package.

Table 4: Rationale for Extended Security Functional Requirements

Extended Requirement	Identifier	Rationale
FTA_TAH_(EXT).1	TOE Access History	This PP does not require the TOE to contain a client. Therefore, the PP cannot require the client to display a message. This requirement has been modified to require the TOE to store and retrieve the access history instead of displaying it.

6 SECURITY REQUIREMENTS

6.1 Additional Security Functional Requirements to The Base DBMS PP

This section defines the functional requirements for the TOE that are amended or specified by this extended package.

Functional requirements in this extended package were drawn directly from Part 2 of the CC [1b], or were based on Part 2 of the CC, including the use of extended components. These requirements are relevant to supporting the secure operation of the TOE.

Table 5: Additional Security Functional Requirements

Functional Components	
FTA_TAH_(EXT).1	TOE access history

TOE Access (FTA)

FTA_TAH_(EXT).1 TOE access information

FTA_TAH_(EXT).1.1

Upon a session establishment attempt, the TSF shall store

a. the [date and time] of the session establishment attempt of the user.

b. the incremental count of successive unsuccessful session establishment attempt(s).

FTA_TAH_(EXT).1.2

Upon successful session establishment, the TSF shall allow the [date and time] of

a. the previous last successful session establishment, and

b. the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the previous last successful session establishment

to be retrieved by the user.

6.2 Security Functional Requirements Refined from The Base DBMS PP

Table 6: DBMS PP Security Functional Requirements modified by this EP

Functional Components	
FAU_GEN.1	Audit Data Generation

Security Audit (FAU)

FAU_GEN.1 Audit data generation

Table 8, auditable events, given in the [DBMS PP] is refined to add the following entry.

Column 1: Security Functional Requirement	Column 2 Auditable Event(s)	Column 3 Additional Audit Record Contents
FTA_TAH_(EXT).1	**None**	**None**

6.3 Rationale For The Additional TOE Security Functional Requirements

The following table provides the rationale for the selection of the security functional requirements. It traces each TOE security objective to the identified security functional requirements.

Table 7: Rationale for TOE Security Functional Requirements

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS_HISTORY The TOE will store information related to previous attempts to establish a session and make that information available to the user.	FTA_TAH_(EXT).1	The TOE must be able to store and retrieve information about previous unauthorized login attempts and the number of times the login was attempted every time the user logs into their account. The TOE must also store the last successful authorized login. This information will include the date, time, method, and location of the attempts. When appropriately displayed, this will allow the user to detect if another user is attempting to access their account. These records should not be deleted until after the user has been notified of his/her access history. (FTA_TAH_(EXT).1)

6.4 Rationale for Satisfying All Security Functional Requirement Dependencies

This extended package does not contain any additional or amended SFRs that have dependencies.

6.5 Security Assurance Requirements

This extended package neither adds to nor alters the security assurance requirements given in [DBMS PP].