Technical Report

Application note on static binding

Version 1.0

2012, the 19th of July

Version history

Version	Date	Editor	Description
1.0 RC1	02-07-2012	A.Feraud	Initial version
1.0 RC2	13-07-2012	A.Feraud	BSI comments integration
1.0	19-07-2012	A. Feraud	Public release

Content

1 Introduction

Despite only the dynamic binding was retained by EU commission for any eMRTDs to be issued in Schengen area after the end of 2014, there are on the field European eMRTDs using static binding. They may be issued until the end of 2014 ([R2]) and shall be valid for their whole life time, that may end up in 2024 (depending on the type of documents).

As stated in [R2] §3.5, static binding must not be used in newly issued document.

This document aims at providing clarifications about how the interoperability between an inspection system (presuming dynamic binding shall be used) and an eMRTDs supporting static binding shall be reached.

Throughout this application note, PACE refers to PACEv2 as defined in [R4].

1.1 Reference documentation

The following documentation serves as a reference for this application note:

[R1] ICAO 9303 Edition 6 Part 1, Part 2 and Part 3

[R2] Technical Guideline TR-03110-1 “Advanced Security Mechanisms for Machine Readable Travel Documents - Part 1: eMRTDs with BAC/PACEv2 and EACv1”, Version 2.10, March 2012

[R3] RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

[R4] ICAO Technical Report “Supplemental Access Control for Machine Readable Travel Documents”, Version 1.01, November 2010

1.2 Terminology

The key words "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in [R3].

MUST	This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase „SHALL NOT“, means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications SHOULD be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the adjective „OPTIONAL“, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced

	functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

2 Case 1 : use of the retry sequence

The inspection system shall first try to perform a PACE followed by an EAC authentication with the eMRTD using the dynamic binding. In case an error is thrown in the Terminal authentication step (TA), a retry sequence shall be performed (as mandated in [R2] §3.5).

The following retry sequence shall be used by inspection systems:

- Reset the eMRTD by switching off the field and switching in on again
- The PACE protocol shall be performed
- The EAC shall be performed using static binding

3 Case 2 : explicit declaration to the inspection system

The eMRTD may as well indicate to the inspection system it supports the static binding, through an informative structure stored in the DG14 (**`SecurityInfo`**). This method allows the inspection system to perform directly the PACE followed by the EAC with static binding, without using the retry sequence.

To indicate support of static binding, **`SecurityInfos`** (stored in DG14) may contain the following entry:

- At most one **`StaticBindingInfo`** MAY be present.

`StaticBindingInfo` : This data structure provides indication that static binding is supported by the eMRTD

- The object identifier **`protocol`** SHALL identify the static binding.
- The integer **`version`** SHALL identify the version of the protocol. Only version 1 shall be used.

```
id-SB OBJECT IDENTIFIER  ::=  {
```
iso(1) member-body(2) fr(250) type-org(1) organisation(175) Smartcard-Standard(3) Smartcard-Standard-ID(1) PACE-EAC-Staticbinding (1)
```
}

StaticBindingInfo ::=  SEQUENCE  {
      protocol  id-SB
      version    INTEGER,   -- MUST be 1
}
```