P1502 HA 2.0

BankID HA 2.0 Impact on Merchants (summary)

Version 1.11

Date: 12.05.2016

TLP; Green (Internal)

TABLE OF CONTENTS

2 CHANGE LOG 3

3 INTRODUCTION 3

4 BANKID WITH A NEW HA 2.0 SECURITY INSTRUMENT 4

4.1 Overall flow of a BankID transaction 4

4.2 The user experience for security instrument selection in the BankID Web-client has changed 5

4.3 Implementations across BankID issuers may vary 5

4.4 Testing by merchants 5

5 PARTS OF THE BANKID NOMENCLATURE USED BY MERCHANTS MAY NEED TO BE REDEFINED 6

6 BEYOND HA 2.0 6

7 DEPLOYMENT DATES 6

8 CONTACT POINTS 6

9 REFERENCES 6

2 CHANGE LOG

VERSION	DATE	BY	CHANGE DESCRIPTION
0.1	29.02.16	Thorbjørn Sundbøe	First draft
0.2	02.03.16	Thorbjørn Sundbøe	Second draft after internal review in BankID Norway
1.0	09.03.16	Thorbjørn Sundbøe	Updated after review by Nets
1.1	28.04.16	Thorbjørn Sundbøe	Added Ch. 4.2, updated Ch. 7, other minor changes
1.11	12.05.16	Thorbjørn Sundbøe	Updated Ch. 7 with revised deployment date

3 INTRODUCTION

The One Time Password (OTP) step in BankID represents the possession factor ("something the user has") in BankID's two-factor authentication scheme. Each issuing bank is responsible for this factor for its own end-user customers. The HA 2.0 project at BankID Norway has the following prime goals:

- Reducing the dependency on physical authenticators by introducing support for new possession factors;
- Enabling BankID issuers to simplify and improve the user experience and to reduce the risk of OTP phishing by transferring authentication values without the need for user input.

HA is the Norwegian word for HAVE, hence the project name HA 2.0. The HA 2.0 project will deliver in two phases (HA 2.0 and HA 2.1 deliveries; please note that the timeline for the latter has not been decided). This document focuses on the initial HA 2.0 delivery.

In short, the HA 2.0 project adapts the BankID infrastructure and Web-client, enabling the issuing banks to offer their customers new, software-based possession factors for use with BankID. Initially this will represent a complement to the current physical authenticators, scratch cards, soft-OTP factors and BankID-on-Mobile-as-OTP solution (BIMOTP). Eventually it may have the potential to replace such legacy factors. The current and new possession factors are jointly referred to as *security instruments* in this document.

The new security instruments enabled by this project will most likely take the form of a native software app provided and provisioned by the issuing bank for use on a smartphone or tablet device. The app implementations are expected to offer a variety of user experiences across BankID issuers. These new possession factors are either referred to as *HA 2.0 security instruments* or simply *HA2 apps* in this document.

Until now, only a smaller portion of the total BankID customers have had multiple security instruments to choose from (typically only those who have more than one BankID certificate and/or those who have BankID-on-Mobile-as-OTP). As BankID issuers roll out HA 2.0 security instruments, an increasing portion of BankID end-users will get multiple such instruments to choose from in the BankID Web-client. This has the implication that a larger portion of the BankID customer base will be faced with dialogs in the Web-client to select/switch the preferred security instrument in any particular context.

BankID merchants that are banks should note that risk data and alarms exposed over the data-to-merchant interface will use additional inputs from the HA 2.0 security instruments. Other BankID merchants are not affected by HA 2.0 in such a way that they must adapt their technical implementations. However, the introduction of HA 2.0 does introduce changes at the issuer end, in the BankID client and hence also at the end user’s end.

4 BANKID WITH A NEW HA 2.0 SECURITY INSTRUMENT

4.1 Overall flow of a BankID transaction

The diagram below illustrates the overall flow of a BankID transaction with a new HA 2.0 security instrument.

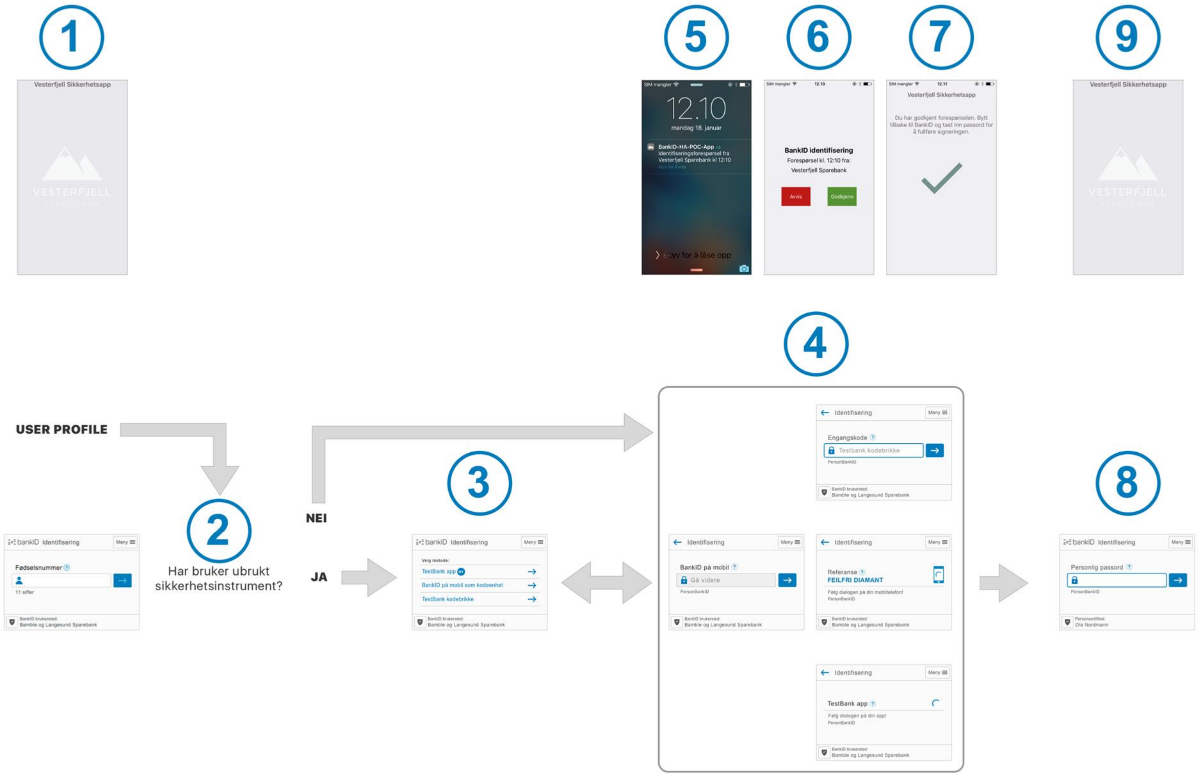

Figure 1: Overall flow of a BankID transaction (for illustrative purposes only, actual implementation will differ).

- Step 1. The transaction is initiated by the end user in the merchant’s application.
- Step 2-4. The flow in the BankID Web-client, prior to the point where the end user interacts with the new HA 2.0 security instrument.
- Step 5-7. An example flow within a HA2 app. Please note that issuer implementations will vary.
- Step 8. The BankID Web-client password dialog. Please note that this step is unaffected by HA 2.0.
- Step 9. Return to the merchant’s application, the BankID transaction has ended.

4.2 The user experience for security instrument selection in the BankID Web-client has changed

Step 2 in the previous section shows that new logic has been implemented in the BankID Web-client. The logic applies to legacy as well as HA 2.0 security instruments and conditionally displays Step 3 (the “HA selector”) or moves directly to Step 4 in the flow. Furthermore, the user experience for security instrument selection, Steps 3 and 4, has changed. The HA selector will be displayed when the user possesses multiple security instruments, and one or more of these have never been used[1] for a BankID transaction (be it legacy, BIMOTP or HA2 app). The HA selector will *not* be displayed in other cases; rather, the last used security instrument will be automatically selected and the BankID Web-client advances directly to Step 4.

Please note that the mentioned changes will materialize in the BankID Web-client as soon as the release has been put into production (see chapter 7), regardless of HA2 roll-out status among BankID issuing banks. In this context it is noteworthy that there is a substantial number of BankID-on-Mobile users who have never used their BIMOTP security instrument. This can be mainly attributed to the fact that BankID issuing banks automatically provision BIMOTP when they issue BankID-on-Mobile for a particular user. These users will see Step 3 until they have attempted to use BIMOTP after HA2 has been released.

4.3 Implementations across BankID issuers may vary

As mentioned earlier, issuers are expected to offer different user experiences. We expect that these variations will move roughly along the following lines:

- Some issuers may restrict the end-user to use the HA2 app on a single device, whereas others may allow multiple device usage. Please note that in the latter case, the BankID Web-client does not know whether the end-user in question has activated multiple HA apps (i.e. the BankID Web-client does not expose multiple HA2 apps to the end-user); this is solely handled at the issuer’s end;
- Some issuers may require app authentication, e.g. in the form of a PIN code or biometry such as fingerprint, whereas others may not;
- Some issuers may start the HA2 app automatically on the user’s device, whereas others may opt for manual startup by the end-user. Please note that in cases where the merchant application and the HA2 app run on a single device, the end-user may in some cases encounter difficulties to return to the merchant’s application after the operation in the HA app has completed (due to app focus issues on the device in question);
- Issuers also have the possibility of feeding some specific content into one of the BankID Web-client dialogs if they so wish. Some issuers may take this opportunity, whereas others may not. Leveraging this option will provide instructions to the end-user that is tailored to the specific user-experience resulting from the HA2-solution from the issuers.

Merchants should consider the implications of the points above.

4.4 Testing by merchants

Merchants that use an automated test rig/framework must consider if their tests need to be updated in order to support the changes in the BankID Web-client dialogs and flow, as described in Figure 1. Please refer to the BankID Web-client Web-UDD viewer for further details.

[1] “Never used” actually means that the user has not previously *attempted* to use the security instrument in question.

See section 7 for when merchants may start testing/verifying their BankID implementations with HA2.0 in the pre-production environment.

5 PARTS OF THE BANKID NOMENCLATURE USED BY MERCHANTS MAY NEED TO BE REDEFINED

The common case with current security instruments is that the end-user is provided with a code that must be entered into the BankID Web-client. The new HA 2.0 security instruments enabled by this project work inherently different in the sense that they do not require the end-user to enter a code into the BankID Web-client (individual issuers may however require app authentication, as mentioned above). This can be illustrated by the commonly used legacy association of BankID with OTP, giving rise to the term "BankID with one time security code". With the introduction of HA 2.0 this designation will no longer work.

The new HA apps will in most cases be issued on mobile devices. A possible complication is that end-users may not be able to distinguish the current BankID on Mobile with the new HA2 on mobile.

BankID merchants should assess these changes for possible implications at their end on how BankID is designated, explained and communicated in conjunction with the merchant solution.

6 BEYOND HA 2.0

As mentioned, the HA 2.0 project will deliver a second release, HA 2.1, after HA 2.0 has been put into production. The timeline for HA 2.1 has not been decided. HA 2.1 will introduce additional options for the issuers, including support for new start/return alternatives between the BankID Web-client and the issuer's HA2 app. One of these alternatives, "local URI", may require changes to the merchant's technical implementation when used for automatic return from the HA2 app to the merchant application. This and other impacts of HA 2.1 on merchants will be described in the HA 2.1 version of this document.

7 DEPLOYMENT DATES

Pre-production: 30.05.2016
Production: 17.08.2016

8 CONTACT POINTS

BankID merchants or issuers may use the following contact point in case of any questions regarding the content of this document or the HA 2.0 project: ha2.0@bankid.no

9 REFERENCES

Banks that are both BankID merchants and issuers, should also read the following documents:

- BankID HA 2.0 Issuer implementation considerations;
- BankID HA 2.0 Service Interface Specification;
- BankID HA 2.0 Fraud Detection Data.