

BankID COI White Paper

Date: 05.09.2005

Version: v1.0

Contact person: Mr. Brynjel Johnsen
brynjel.johnsen@bbs.no
Bankenes Betalingssentral AS

Copyright

Copyright © 2002-2004 Bankenes BetalingsSentral AS (BBS), Organisation Number N- 975 946 231, Haavard Martinsens vei 54, N- 0045 OSLO, Norway.

Disclaimer

This document is awaiting approval from the BankID Coordination Group ("BankID Samarbeid"). BBS does not guarantee for the correctness of the content in the document until it is approved.

**BBS
N- 0045
NORWAY**

Summary

This document describes the functionality in the BankID Common Operational Infrastructure (COI), presents an overview of various components and their operations.

The BankID COI consists of central and distributed infrastructures. Central infrastructure consists of components, which make it possible to issue, use and validate BankID certificates. This includes the Registration Authority (RA), issuing and revoking functions (RA/ CA), validation function (VA) and the Test & Activation (T&A) service. In addition, the central infrastructure consists of central services for bank-stored BankID solution for key storage and signing functions.

Distributed infrastructure consists of functions that are necessary for the administration of BankID, customers' use of BankID (for identification and signing) and to establish trust among the end users in BankID.

BankID can be used for online identification and signing based on this COI.

BankID identification consists of a process where the customer (certificate holder) is requested to identify towards a BankID merchant (certificate receiver). Depending on the kind of BankID (i.e bank-stored or locally stored) that the customer chooses to use, a dialogue is initiated where the customer is asked to type-in his/ her Social Security Number (SSN), the BankID to be used (bank-stored or locally stored), static password and one time password (OTP). The dialogue presented to the customer is always identical and is independent of the merchant (but is not identical when using bank stored or local stored BankID).

BankID Signing can be completed regardless whether the customer previously has identified himself/ herself or not. Depending on the type of BankID key storage (bank-stored or locally stored), a dialogue is initiated where the customer is presented to the information to be signed. The customer is thereafter asked to type the information regarding identification number, which BankID to be used, static password and eventually one time password. The dialogue presented to the customer is always identical, independent of merchant (but is not identical when using bank stored or local stored BankID).

1	INTRODUCTION	6
1.1	Target audience	6
2	TERMINOLOGY	6
2.1	Overall concept description	8
3	ABBREVIATIONS	10
4	BANKID CERTIFICATE POLICY	11
5	ABOUT COMMON OPERATIONAL INFRASTRUCTURE FOR BANKID	11
5.1	The BankID Community	11
5.2	Overall principles	12
5.3	Choice of technology	12
5.4	Security	12
6	SYSTEM ARCHITECTURE FOR BANKID COI	12
6.1	Central infrastructure	13
	BankID Root-CA	14
	BankID Level 1-CA	14
	Order and Distribution System (ODS)	14
	BankID Bank stored Central Servers	14
	Validation Authority	14
	BankID Test and Activation Site	15
	Certificates	15
	Key Store	15
	Types of certificates	15
	Database for Unique Identifier (PID)	15
6.2	Distributed infrastructure	15
	BankID Level 1 - RA	16
	BankID Local stored client	16
	BankID Bank-stored client	16
	One Time Password (OTP) mechanism	16
	BankID Server Java	17
	BankID Server C	17
	Certificates	17
	Interruption and disaster solution	17
7	PROCESS	18
7.1	Functions in use of BankID (Key Features)	18
	BankID client and Server	18
	Access to BankID private keys	18
	Verification of the parties identity (certificates)	19
	Validation of certificates status	19
	Distribution of additional information	19

Digital Signature with SDO	19
BankID Document Organiser	19
7.2 Local stored BankID	19
Order	19
Test & Activation	20
Identification	20
Signing	21
Revocation, Suspension and un-suspension	21
Renewal	21
7.3 Bank-stored BankID	22
Ordering	22
Test	22
Identification	22
Signering	23
Revokation, Suspension and Un-suspension	23
Renewal	23
7.4 Merchant	24
Ordering	24
Test & Activation	24
Identification	24
Signing	24
Revocation, Suspension and Un-suspension	24

1 Introduction

This document has been prepared to give a brief overview of all the functions and components in the BankID Common Operational Infrastructure (COI). This White Paper is not a technical document. Detailed description of the numerous components is given in the technical reference documentation within the BankID Server package. A CD with documentation and software is licensed and can be ordered from all BankID member banks (issuing BankID certificates).

1.1 Target audience

The target audience is anyone who wishes to understand the BankID COI operations, components and functions. As BankID is based on implementation of the PKI technology, the use of technology-related expressions is inevitable. Consequently, we have listed the most common concepts and abbreviations at the beginning of this document.

2 Terminology

- BankID** BankID is used as common denomination of certificates for physical persons and merchants with associated private keys, issued by a BankID issuing bank. BankID will consist of, but not be limited to, authentication and signing certificates with associated keys.
- Client** Client is the BankID software used by certificate holder in order to use his/ her BankID certificate for identification and signing.
- Locally stored** Locally stored relates to a solution where the customer installs BankID client on a computer. The customer's BankID with encryption keys, certificate and software are stored on the customer's computer locally and are protected with a static password known only to the customer. The customer's BankID may be imported and exported (i.e. transferred to another computer) and deleted when required.
- Bank-stored** Bank stored relates to a solution where the customer can use his BankID from all computers without installing software and digital certificate on a permanent basis. The customer's certificate with the associated keys is stored in a central key store. The customer gets access to his/ her Bank stored BankID by typing his SSN, one time password and static password.
- BankID Server** A set of cryptographic functions to be installed on a website in order to accept BankID as a digital ID and digital signature. The BankID Server exists in two versions, C-version and Java-version.
- SDO** A standardised signature format comprising the signed data, the signature of the parties and result of VA request at the time of signing. BankID SDO is aligned with ETSI TS 101 733, Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats, version 1.5.1, December 2003
- SSN** Social Security Number. Consists of birth date and a 5 digit control number. Format: DDMMYY-XXXXX

- PID** Personal Identifier is a unique identifier generated by the BankID COI for the end-users for use within the BankID community. Unlike the SSN (identifier), a PID can be changed for reasons of online privacy.
- OTP** One Time Password. It is used in the Bank-stored BankID.

2.1 Overall concept description

The Norwegian banking sector has established the BankID Community under the governance of The Norwegian Financial Services and Savings Bank Associations. In its first phase, BankID will be used for electronic identification and signing in Internet banking services and other web sites (offering third party online services). The overall goal is to use BankID in securing electronic services in the business segments, public-administration, electronic-commerce/ shopping and other online-transactions.

A coordinated infrastructure is the basis for issuance and usage of BankID. The infrastructure consists of common elements: Inter-bank regulation, trademarks, policies and procedures, security requirements, standards and supplementary profiles, as well as various technical components. This will secure: interoperability between the technical components in the BankID infrastructure, user-friendliness/ security, as well as simple integration and use of BankID in electronic services. The Norwegian Banks Payment and Clearing Centre (Bankenes Betalingsentral or BBS) has developed and is now operating the BankID Common Operational Infrastructure (COI).

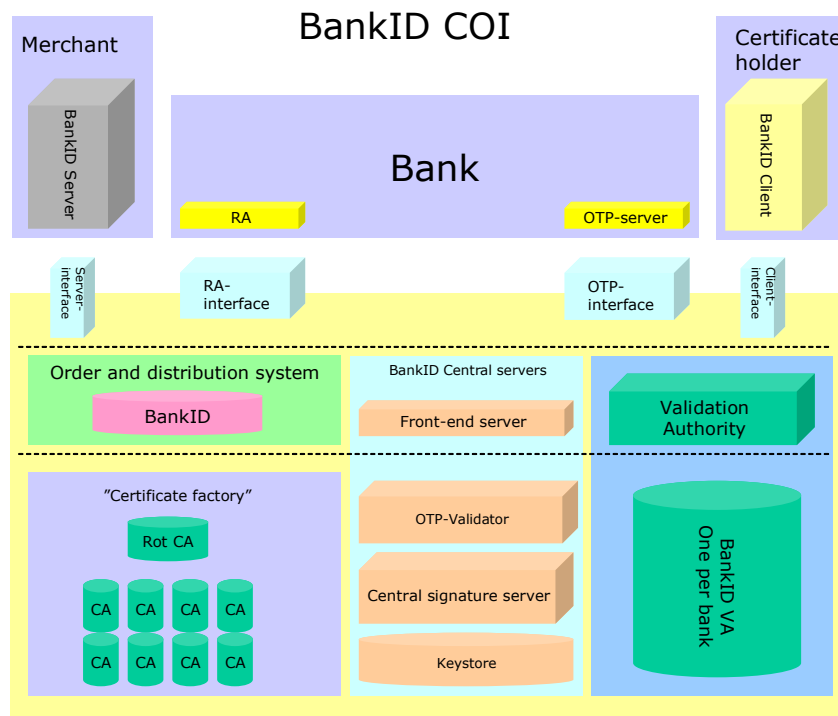


Illustration 1 – BankID infrastructure overview

BankID is based Public Key Infrastructure (PKI). The technology is based on asymmetric cryptography and employs a key pair, a private (secret) and a public key, used to secure the transactions. In addition, the certificate, i.e., “electronic ID” is used to link the key-holders identity to the public key. The method describes how the keys and associated certificates are issued and used.

PKI consists of four central roles and these are defined as follows:

1. **Certificate holder/owner:** A person (physical or legally) who possess a BankID and who uses BankID for identification and/or signing.
2. **Merchant:** A website, for example an Internet banking service or merchant, accepting BankID identification and/or signing.
3. **Certificate issuer:** An RA/ bank issuing BankID. Maintenance of BankID throughout its lifetime (issuing, revoking, renewal). A bank is always the RA and may also be CA. Some banks share same CA.
4. **Certificate validation:** A Service provided by issuers/ CAs for checking validity of certificates.

When accepting BankID as digital ID (or signature), the merchant shall send a request to its bank requesting proof of validity of the certificate holder's BankID. If another bank has issued the certificate holder's BankID, the merchant's bank shall ask the issuer's bank whether the certificate in question is valid or not.

3 Abbreviations

BSK	Bankenes Standardiseringskontor (Norwegian Banks' Standardisation Office)
CA	Certificate Authority (issuing and revoking certificates)
COI	Common Operational Infrastructure
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DNS	Domain Name System
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
ODS	Order Distribution System
OTP	One-Time password
OWF	One Way Function
PID	Personal Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKCS	Public Key Cryptographic Standard
PSE	Personal Security Environment
RA	Registration Authority
RNG	Random Number Generator
SDO	Signed Data Object
SSL	Secure Sockets Layer
SSN	Social Security Number
UID	User ID
USP	User Static Pass-phrase
VA	Validation Authority

4 BankID Certificate policy

Security requirements for the BankID Service is set by BSK and documented in policy-documents for the different types of BankID (personal certificates (local stored, bank stored), certificates for employees (locally stored, bank stored) and merchant certificates. The document includes requirements for:

- Responsibility and confidentiality
- Request for registration of customer
- Ordering, issuance and usage of BankID
- Requirements and procedures regarding revocation and suspension
- Physical and logical security in the BankID infrastructure
- Technological security
- Certificate profiles

The BankID COI is based on the requirements set by BSK. All questions regarding policy, security requirements and supplementary regulation shall be addressed to BSK.

5 BankID COI

5.1 BankID Community

BankID is based on a coordinated infrastructure developed by the Norwegian banking sector through the BankID Community, under the governance of The Norwegian Financial Services and Saving Banks' Associations.

The BankID Community is responsible for the development and administration of a **coordinated infrastructure** in the banking industry.

Participants in the BankID Community are:

- **Banks:** The development of the BankID Infrastructure is performed of different work groups in which the banks have an active role.
- **BSK:** BSK has the responsibility for setting the policy, standards and security requirements. BSK has also a control responsibility regarding compliance with these requirements. BSK has appointed a technical coordinator for BankID.
- **The Norwegian Financial Services Association and the Norwegian Saving Banks Association:** Preside over and organise the work with the BankID Infrastructure, through the common organisation, which is established for the infrastructure within transaction of payments. A BankID coordinator is responsible for coordinating the activities in the BankID Community across various stakeholders.

The BankID Community has given **The Norwegian Banks' Payment and Clearing Centre (BBS)** the responsibility to develop the Common Operational Infrastructure (COI).

5.2 Overall principles

BankID uses "Public Key Infrastructure (PKI)". This technology is based upon asymmetric cryptography, which enables parties not already having a trusted relationship to establish secure communication and perform secure transactions on the web. This is made possible when both the parties have a trusted relationship mutually with a third party. The trusted third parties in BankID community are the two parties' respective banks. If the two parties have different banks, the trust relationship is regulated with agreements between the banks of the two parties. The trust between banks, in-turn, is regulated through "Regulations for BankID" in the Inter-bank regulations.

5.3 Choice of technology

PKI is the most common technology, which enables a "many-to-many" trusted relationship, regardless if the parties have prior knowledge of each other or not. Although BankID makes use of technologies from different vendors, Cybertrust has supplied the platform used in the BankID COI.

5.4 Security

The BankID COI makes use of strong encryption in all security functions. In the central infrastructure the HSMs are used to create keys and perform the cryptographic operations. No encryption keys are less than 1024 bits RSA.

6 BankID COI Architecture

The trust chain in the BankID is founded in a Root-CA jointly owned by The Norwegian Financial Services and Saving Banks Associations. The Root-CA owned by the Bank Associations issues certificates to the level 1 CA's for the BankID-member banks. The BankID Infrastructure is based on "Regulations for BankID", which among other things implies intercommunication between all banks in Norway issuing BankID.

Each bank will act as RA. Issuers of certificates are banks and groups of banks.

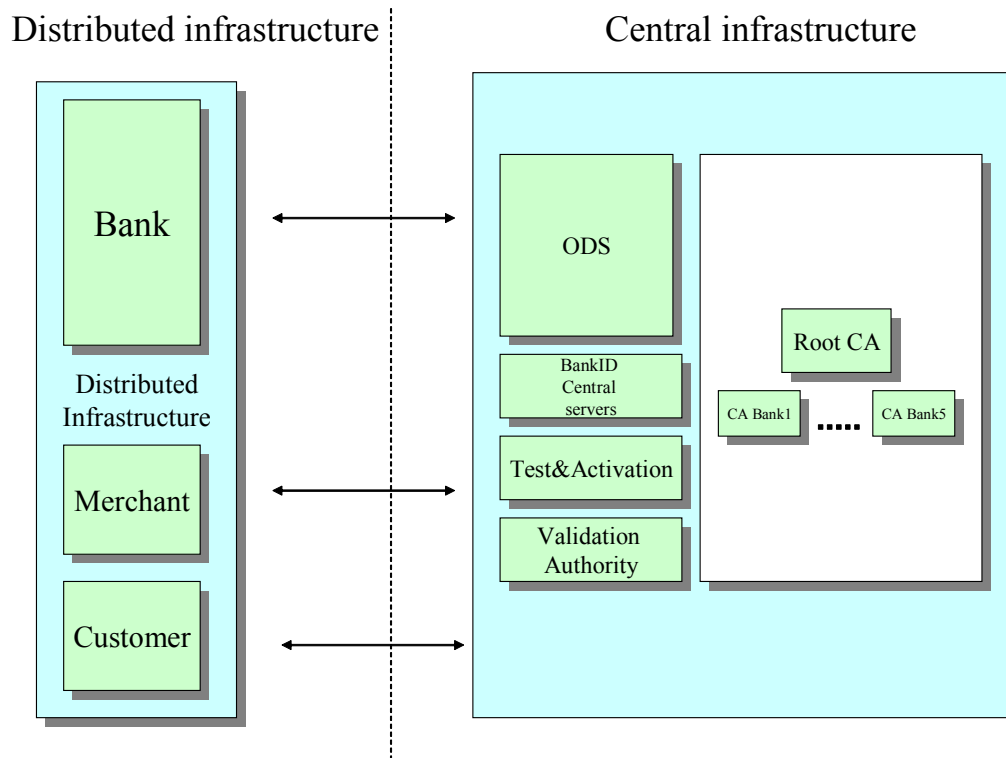


Illustration 2 –Showing how the different parts of the COI are connected

The system architecture consists of central infrastructure, registration authority, client and merchant server components. These are described in the following chapters.

6.1 BankID Central infrastructure

Central infrastructure covers the functions, which are not executed in the clients (i.e. certificate holder) or at the merchant (i.e. certificate receiver). The infrastructure also includes necessary interfaces to the distributed infrastructure.

Central infrastructure includes the following functions:

- Certificates ordering
- Certificates issuing
- Certificate revocation (permanent)
- Certificate suspension (time limited)
- Certificate un-suspension (opening of time limited suspended certificates)
- Certificate renewal
- Certificate validation (OCSP)
- One time password validation
- Central storage and use of private and public keys (Bank stored BankID)
- Communication of certificates status information
- Administration of certificates and additional information

Root-CA

BankID Root-CA is owned by the two bank associations in Norway. The purpose of the BankID Root-CA is to issue certificates to the CA's in order to give the banks a common foundation for issuing certificates to their customers. BankID Root-CA is a common trusted point for all the users of BankID. The certificate of BankID Root-CA is valid for 26 years and is renewed after 14 years.

The following function is available:

- BankID Root-CA

Level 1-CA

A BankID Level 1-CA is owned by a single bank or a bank group and it is used to issue and revoke certificates to customers in a participating BankID bank. Level 1-CA issues Certificate Revocation Lists (CRLs) with certificates, which are revoked and makes the CRLs available to the Validation Authority (see below). Level 1-CA certificates are valid for 12 years.

The following function is available:

- BankID Level 1-CA per participating bank/ bank group

Order and Distribution System (ODS)

In order to simplify the administration of certificates issued by the different Level 1-CAs, an Order and Distribution System (ODS) is implemented. ODS is a database with an interface towards several components in the central infrastructure and contains numerous functions for administration and application of the BankID certificates.

The following functions are available:

- ODS Database
- BankID RA/ODS interface
- Interface towards other components (CA, Bank stored central servers)

Bank stored Central Servers

Bank stored BankID is based on the central storage and use of end-users' BankID certificates and keys. In order to make this possible, a range of functions and components enabling the storage and usage of certificates and keys are implemented.

The following components are available:

- BankID Server Front-end
- BankID Server Database
- BankID Central Signing Server
- BankID Bank Stored Key Store
- BankID Authentication Server
- Interface towards the one time password mechanisms

Validation Authority

The BankID COI has implemented online validation system (Validation Authority - VA). The VA receives CRL (list of revoked BankID certificates) from the Level 1 CAs and delivers a function for certificate validation available to both certificate holders and merchants.

The VA also has a function to deliver additional information to the authorised merchants about certificate holders. This function is only available for those merchants who have a legal right to obtain such

information and if the merchant has entered into an agreement with its bank. Available additional information are:

- Social Security Number (SSN) of the certificate holder
- Account number of the certificate holder

Test and Activation Site

BankID Test and Activation Site (T&A) has several functions for different type of BankID. All key-store types can be tested and diagnosed at this site. For the locally stored BankID, this is the site where new certificates can be downloaded and where certificate holder activates his/ her BankID. The T & A Site is available to both the end-user and merchants. Administration of all types of personal BankIDs may also be performed on the T & A Site.

Certificates

All components in the central infrastructure have their own certificates and key pairs for secure and safe communication.

Key Store

A key store is a secure location where the certificates and corresponding keys are stored and used. The following key stores exist in the current BankID:

- Bank stored
- Locally stored

Types of certificates

Different types of certificates are implemented to make possible the use of BankID in numerous connections. The following types of certificates exist in today's version of BankID

- Personal certificates – used by private persons
- Employee certificates – used by persons acting on behalf of a enterprise or organisation
- Merchant certificates – used by web sites

Personal Identifier (PID)

Each personal certificate has a unique identifier (PID). This identifier is unique for each person and exists in all the certificates issued to the person, independent of who has issued the certificate. In this way a certificate holder can identify himself/ herself towards the web site at every visit, independent of which BankID in use. In the central infrastructure there is a database, which assures that the end-user gets the same PID in all his/ her certificates. However in order to secure the personal protection, the end-user may choose to have a new PID when requesting a new certificate.

6.2 Distributed infrastructure

Distributed infrastructure consists of components enabling the usage of BankID for the end-user, merchant or bank. Distributed infrastructure includes the following functions.

- The banks' administration functions for BankID
- BankID for authentication and signing functions
- Acceptance of BankID

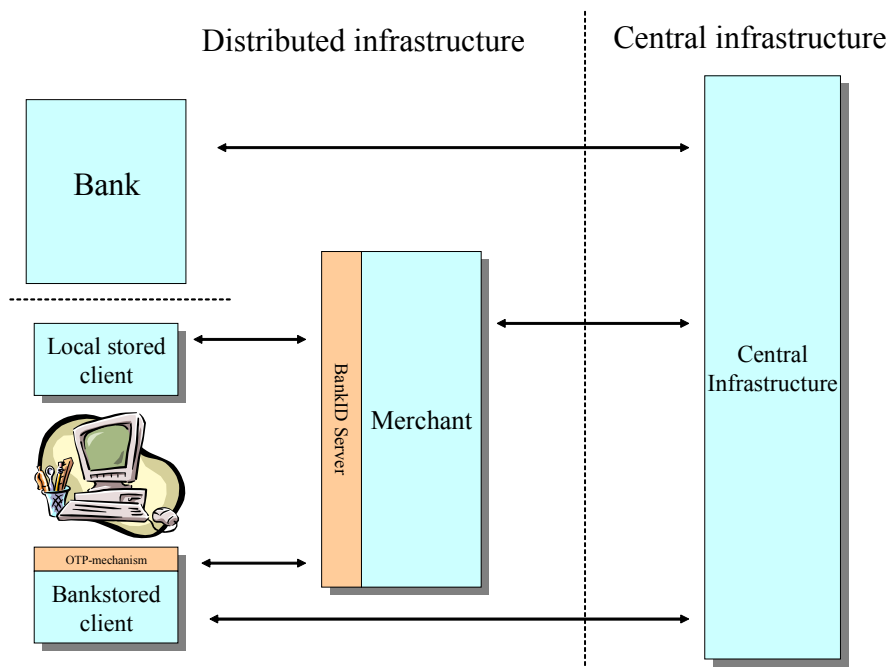


Illustration 3: Showing the Distributed and Central Infrastructures in BankID

Level 1 - RA

To issue the certificates from a Level 1-CA, bank must set up a Registration Authority (RA). This is a function for registration and administration of certificates issued by the CA used by the bank. The RA should normally be integrated into the ordinary customer service management systems and communicates via a standard interface towards the ODS, offered by BBS as a central certificate administration system.

Locally stored client

Locally stored BankID client is a Java-applet installed at the end-users personal computer together with his/ her certificate. The client is downloaded from the Test & Activation Site at the same time as activation of BankID and contains all PKI functionality for authentication and signing towards BankID merchants. In order to get access to these functions, the end-user must enter username and static password.

Bank-stored client

BankID Bank-stored client is a Java-applet downloaded by the end-user to his/ her local computer each time s/he wants to use BankID for authentication and signing. The client is downloaded from the Bank-stored central servers and contains only the necessary functions to access the PKI functionality in BankID Bank-stored servers. In order to access these functions, the end-user must enter Social Security Number, static password and one-time password.

One Time Password (OTP)

The use of Bank-stored BankID requires that the end-user possesses an OTP-device issued by the bank. Banks may choose an OTP device and mechanism, subject to approval by The Norwegian Banks

Standardization Office (BSK). The OTP device provides the end-user with a unique password for a limited time.

The bank will administer the one time password system. The OTP-system shall have a function for communication with Bank-stored central servers through the OTP interface towards the BankID COI.

BankID Server (Java)

BankID Server (Java) is a collection of functions implemented at merchants having entered into an agreement with his/ her bank to accept the end-users BankID certificates for authentication and/or signing. The software is written in Java programming language and consists of all the necessary PKI and communication functionality to complete a transaction with the end-user and BankID Validation Authority.

BankID Server (C)

BankID Server (C) is a collection of functions implemented at merchants having entered into an agreement with his/ her bank to accept the end-users BankID certificates for authentication and/or signing. The software is written in C programming language and consists of all the necessary PKI and communication functionality to complete a transaction with the end-user and BankID Validation Authority.

Certificates

In order to protect the communication between the banks' RA-function and ODS, the CA issues a SSL certificate to each RA. The communication between the RA-function and ODS is encrypted in two-way SSL in a secure dedicated network.

For Locally stored BankID, the end-user certificates and keys are stored as a PKCS#12 file, protected with BankID encryption in connection to the BankID client. For Bank stored BankID the certificates and keys are stored encrypted in a central key store. Both types of certificates are issued by the Level 1-CA belonging to the banks.

A merchant may either store the certificate as a file (encrypted PKCS#12) or make use of a Hardware Security Module (HSM). Both types of certificates are issued by the Level 1-CA belonging to the banks.

Disaster recovery

BankID COI offers solutions for identifying and signing for Internet Banking and also other web sites, which demand secure access, control. To ensure the availability for the system, BankID is designed as a "High Availability" solution with automatic interruption and disaster technology seamlessly transfers operation to a backup system if the main system should fail. Neither the merchants nor the end-users will notice such a situation.

7 BankID in use – process description

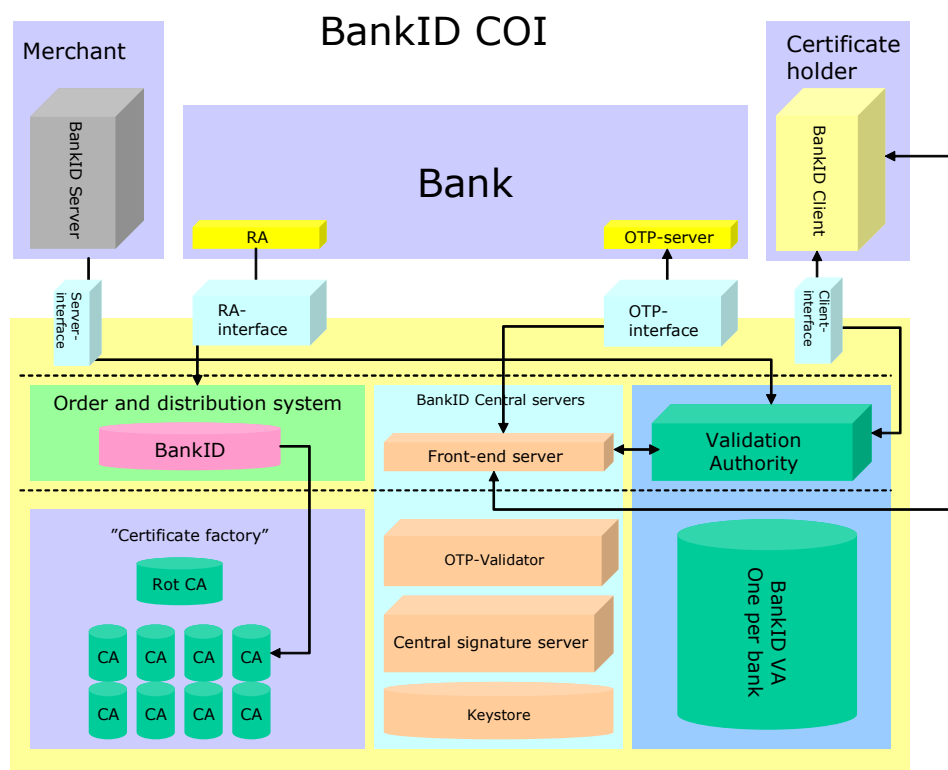


Illustration 4 –Communication between the various BankID COI Components

7.1 Functions in use of BankID (Key Features)

BankID client and Server

All use of BankID certificates and keys assumes that the certificate holder visits a web site, which has been enabled for BankID identification and/or signing through the implementing BankID Server in its web-server/ web-application.

The merchant must implement functions in its web site to initiate the downloading and running of the BankID client in the end-users browser. The certificate holder uses functions in the client to access and use his/ her BankID with associated keys. The web site uses functions in the BankID Server to access and use his/ her BankID with associated keys.

Access to BankID private keys

In order to use his/ her BankID, the certificate holder and merchant must know the “certificate activation data”. The following activation data is necessary for the different key stores:

- Locally stored BankID: Static password (must also possess the certificate and keys)

- Bank stored BankID: Static password and one time password (mechanism to generate one time password is offered by the bank of the certificate holder)
- Merchant certificate: Static password

Verification of identity (certificates)

By using BankID, the parties are enabled to verify the identity of the other party. Each party forwards a challenge to the other to be signed with the corresponding private key of the opposite party before it is returned. When receiving the signed response, the parties are able to verify that the other party possesses a real BankID and may collect information about their mutual identities from the certificate. For physical persons, the information in the certificate also includes a PID, a unique identification number maintained by BankID.

Validation of certificates status

To ensure that the other party's certificate is valid, both parties request status information about the other party's certificate. The parties send a request to the validation authority (VA) and the VA responds whether the requested certificate is valid or not. The VA is updated in real time with information about the certificate status available in the level 1-CA's.

Distribution of additional information

Banks are subject to legal regulations on privacy for the protection of sensitive information, i.e. SSN and hence this information cannot be included in the BankID certificate. It is therefore an established service at the VA for including the SSN of the certificate holder in the OCSP response to the merchant. Only the merchants with legal authority to access/ handle such information have access to this service. Access-control is managed for each merchant by the RA.

This service may be extended to offer further information about the certificate holder at a later stage.

Digital Signature with SDO

BankID offers a function for digital signature. A digital signature is as binding as a handwritten signature and with BankID digital signature the banks assure that the correct certificate holder has signed a document with BankID (provided that the certificate holder has not behaved negligently and thereby compromised his BankID, password and/or one time password mechanism).

In order to secure the storage, retrieval and readability, the (BankID member) banks have established a standardised signature format "BankID Signed Data Object" (BankID SDO). All documents signed by BankID are stored in this format, comprising the signed data, the signature of the parties, and result of the VA-requests at time of signing. BankID clients offer a function for saving the SDO to the certificate - holders hard drive.

BankID Document Organiser

The document organiser offers an easy function for the retrieval and verification of BankID signatures. The end-user may download the application BankID Document Organiser, which searches through the hard drive, showing all BankID SDO's found in a document overview. The organiser can also display the documents and signature information.

7.2 Locally stored BankID

Ordering

This description covers ordering of local stored BankID. Several of the functions below involves both central and distributed infrastructure as described in previous chapters. The customer may order his/ her locally stored BankID through the Internet banking service (as s/he has already been identified by the banks' netbank system) or by a direct appointment in a bank office.

The following procedure describes in steps the ordering process in an Internet banking service:

1. The bank orders a locally stored BankID for the bank customer using the BankID RA interface
2. ODS receives the order and forwards an installation code (shared secret) to the customer (through the Internet bank or another approved channel).
3. The bank customer is redirected to the Test & Activation site, where the BankID Client software is automatically downloaded to the customers' computer. During the installation of locally stored BankID, the bank customer is prompted to enter a static password in accordance with the BankID password regulations (the software only permits passwords following the rules of BSK).
4. After installation, the client will generate public and private keys.
5. Then the customer is asked to type-in the installation code (shared secret).
6. The public key is sent in a certificate request together with the shared secret to the ODS, which compares this information with the original order (from the bank).
7. ODS forwards the certificate to the bank's CA. The bank's CA generates a certificate which is sent to the customer via ODS.
8. The bank customer activates his/ her certificate at the Test and Activation Site. After activation, the BankID is ready to use.

Test & Activation

The activation of BankID certificates is part of the installation process for the locally stored BankID. After activation, the Test- & activation site guides the certificate holder to the test sequence. Test of BankID may be done at any time after activation.

The following procedure is accomplished at testing:

1. Identification is tested by the Test & Activation site. The certificate holder is requested to identify himself/ herself with his/ her BankID. The T & A site validates the certificate at the VA.
2. An automatic test sequence is carried out, checking the status on the client software.
3. The signing function is tested through the users' signing of a test-data. The T & A Site verifies the validity of the signature.
4. All data regarding the tests are logged and the necessary information is presented to the customer.

Identification

This section describes how a certificate holder identifies himself/ herself towards a merchant with a locally stored BankID. Identification with BankID is based on a two-way "challenge-response" mechanism through an encrypted connection (SSL).

1. If the merchant has enabled the function to assure a "Simplified selection of key-store", the Bank-stored client will be downloaded initially. The certificate holder will then enter his/ her SSN before the software checks with central infrastructure, where the key-store is available for the certificate holder. If the certificate holder has only the locally stored BankID or more than one key-stores are available, see section 2 below. In any other case see relevant section for other key-stores.
2. Locally stored BankID client is loaded from local hard drive, is run in the browser, and enters identification-mode. If the end user has a previous version of the client, the most recent client will automatically be downloaded from central infrastructure.
3. The certificate holder will be able to read the name of the merchant in the client (as stored in the merchant's certificate). The client then verifies the certificate chain of the merchant. As part of this process the certificate holder will be prompted to select the correct local stored BankID (a certificate holder may have several locally stored BankIDs). The certificate holder will also be asked to enter his/ her fixed password.
4. During this process both parties identify each other by sending a random value (challenge) to the other party. The other party signs the challenge and returns the signature (response).

5. The locally stored client verifies the signature received from the merchant and sends a signed validation request to the BankID VA (OCSP), which in turn responds with a reply to the request.
6. The Merchant verifies the signature received from the certificate holder and sends a signed validation request to the BankID VA (OCSP), which in turn responds with a reply to the request.
7. The Validation Authority may also reply with additional information about the certificate holder to a merchant, which is enabled and approved to receive Social Security number, or account number.

Signing

This section describes how a certificate holder digitally signs a document. The certificate holder may already have been identified, or identification may be a part of the signing process.

1. Certificate holder enters SSN.
2. If the certificate holder has more than one key-store, s/he would have to select relevant key-store (in the following case a local key-store is assumed)
3. The certificate holder is presented the data to be signed and accepts the contents.
4. If the certificate holder has more than one locally stored BankID, s/he will be prompted to select the correct BankID. Refer section describing the signing process for locally stored BankID.
5. Certificate holder enters a static password.
6. Hash value of the data to be signed is generated, signed by the merchant and sent to client.
7. The client verifies the merchant's signature and signs the hash with the certificate holder's private key.
8. The client validates the merchant's certificate (OCSP)
9. The client sends the signature to the merchant. The merchant verifies the client signature.
10. The merchant constructs SDO and returns the SDO to the client. The Certificate holder may now save the SDO in his/ her hard drive.

Revocation, Suspension and un-suspension

Revocation and suspension are different types of withdrawal (invalidation) of a certificate. In the BankID community, the key difference between these concepts is that while revocation is permanent, a suspended certificate may be un-suspended within 30 days. If not, a suspended certificate will automatically be revoked after 30 days. A BankID certificate may be revoked or suspended if the private key belonging to the certificate is suspected, or factually compromised, or if the information in the certificate no longer is correct. A certificate will normally be suspended if the certificate holder cannot identify himself/ herself properly, i.e., via telephone, e-mail.

1. Revocation or suspension can be initiated by the RA, Issuer or the certificate holder.
2. The certificate holder may request revocation or suspension by telephone to his bank's customer centre, personal visit or by a signed revocation request.
3. The RA will then send a request for revocation/ suspension via the RA-interface to the ODS, which in turn formats and sends the request to the correct CA.
4. The Bank/RA will receive a receipt that the transaction has completed, and can send a message to the certificate holder that his certificate has been revoked/suspended.

Un-suspension may be requested within 30 days and requires proper identification by the certificate holder. The Bank may enable un-suspension via telephone, and electronic online-service (both by using a two-factor by personal appointment).

Renewal

A locally stored BankID is valid for two years. To make it as easy as possible for the certificate holder, BankID COI features an automatic renewal process. In a pre-defined time window prior to the expiration

date, the client will give the certificate holder the option to renew the certificate. If the certificate holder agrees to renew, the following procedure will be initiated.

1. The client generates new keys and a certification request
2. The client signs the request with the certificate holders existing BankID
3. The client sends the signed request to the ODS, via the T & A site
4. The correct CA generates new certificates and sends these to the certificate holder via a secure connection.

7.3 Bank-stored BankID

Ordering

This description covers the ordering process for Bank-stored BankID. Many of the functions mentioned below involves both central and distributed infrastructure described in previous chapters. A Bank customer may order his/ her Bank stored BankID from an online Internet banking service, or by personal appointment to the bank. The following procedure covers online ordering from an Internet banking service

1. The Bank orders a Bank-stored BankID on behalf of the bank customer. The request is sent via the RA-interface to the ODS together with information on the customer's SSN, OTP-device and temporary fixed password.
2. The ODS receives the order and sends a request to the central key-generator to generate the private and public keys for the customer.
3. The private key is encrypted and stored in a secure database, while the public key is sent to the ODS, which in turn forwards it to the relevant CA in a certificate request.
4. After Certificate generation at the CA, the ODS sends the certificate to the certificate database in the central infrastructure. The customer now becomes a certificate holder. The certificate holder will now receive a message that a new BankID has been generated in his name.
5. The certificate-holder may use his/ her Bank-stored BankID when the OTP-device has been received from the bank.

Test

The certificate holder may at any time test and diagnose his/ her BankID. The following procedure is then followed.

1. The certificate holder visits the BankID T & A merchant website. The merchant makes a normal identification of the certificate holder, and validates the certificate.
2. An automatic test sequence will check status on the client software
3. The certificate holder will be asked to sign dummy data.
4. The Test & Activation site will verify the signature and validate the certificate holder's certificate.
5. All data from the tests are logged and presented to the customer.

Identification

This description covers how a certificate holder goes through identification with a merchant, with his/ her Bank-stored BankID.

1. If the merchant has enabled the function for "Simplified selection of key-store" the Bank-stored client will be downloaded initially. The certificate holder will then enter his/ her SSN before the software checks with central infrastructure which key-stores are available for the certificate holder. If the certificate holder has only Bank-stored solution, or more than one key-store is available and certificate holder selects Bank-stored, see section 2 below. In any other case see relevant section for other key-stores.

2. An encrypted connection between the two parties is established. Certificate holder and merchant identify each other by forming and sending a challenge to the other party. The merchant signs the received challenge and returns its response. An encrypted connection between the two parties is established.
3. The certificate holder enters One Time Password and static password.
4. The client sends the passwords, the challenge (received from merchant) to be signed and the signed response from the merchant to the BankID central server.
5. The central server uses the certificate holder's static password to decrypt and access the certificate holder's private keys. The central server also verifies the entered OTP-value against the bank's OTP-system.
6. The central server verifies the signature in the merchant's response and checks validity of the merchant's certificate.
7. The challenge from the merchant is signed with the certificate holder's private key and sent encrypted to the client.
8. The client returns the signed response to the merchant.
9. The merchant verifies the signature in the received response, and checks validity of the certificate holder's certificate.
10. The Validation Authority may also reply with additional information about the certificate holder to a merchant, which is enabled and approved to receive Social Security number, or account number.

Signing

This section describes the signing process of a document by a BankID user using Bank-stored solution:

1. Certificate holder enters SSN.
2. If the certificate holder has more than one key-store, s/he would have to select relevant key-store (in the following Bank-stored keystore is assumed)
3. Certificate holder is presented the data to be signed and accepts the contents.
4. If the certificate holder has more than one Bank-stored BankID, he will be asked to select Bank.
5. At this stage the merchant signs a hash of the data to be signed, and signs the hash with its private key. The merchant sends the signature and the data to the client.
6. The certificate holder enters OTP and static password (if s/he has more than one Bank-stored BankID s/he will be asked to enter OTP in a separate dialogue. Certificate holder selects which BankID to use and enters static password in next dialogue). If the certificate holder has a valid OTP-session (OTP-session is valid for a few minutes), it will not be necessary to enter OTP again.
7. A hash value of the data to be signed is sent to the central server together with static password, OTP (if needed), and the merchant's signature.
8. The central server verifies the OTP (if needed), verifies the merchant's signature, checks validity of the merchant's certificate and uses the certificate holder's static password to access private keys and sign the data.
9. The signature is returned to the client, together with the signing certificate and the result of the VA-check that the central server made on behalf of the certificate holder.
10. The client forwards all these elements to the merchant for signature verification.
11. The merchant creates and SDO, and returns this to the client. The certificate holder may save the SDO to his hard drive.

Revocation, Suspension and Un-suspension

See the procedures for Locally stored BankID in section 7.2.

Renewal

The Bank-stored BankID is valid for two years.

To make it as easy as possible for the certificate holder, BankID COI features, an automated renewal function. In a pre-defined time window prior to the expiration date, the client can automatically renew the certificate holder's certificate.

1. The RA will initiate a renewal procedure in the ODS, by marking the certificate for renewal.
2. The first time the certificate holder uses his BankID after the certificate is marked for renewal, a renewal message will be displayed in the client.
3. Technically, a renewal will imply the same functions as first time issuance, but this is transparent for the certificate holder.

7.4 Merchant

Ordering

Ordering of a BankID merchant certificate is initiated by the merchant by appointment to a bank issuing BankID. Integration of BankID server software can be done by the merchant itself, or by a subcontractor (preferably an authorised BankID partner).

1. The merchant applies to the Bank for a test certificate.
2. After a successful test phase, the merchant enters normal production with a full-BankID production certificate.

Complete procedures for establishing a merchant are documented in the BankID Server package (BankID Implementation Guide). The merchant's private keys may be generated and used in software or in a Hardware Security Module.

Test & Activation

The merchant's certificate are downloaded and activated from the Test & Activation site, very much in the same way as for locally stored BankID. Currently no dedicated test-functions for merchants are available.

Identification

The merchant identifies itself towards the client and the central BankID infrastructure.

Signing

The BankID Server software enables the merchant to sign challenges, data (documents) and OCSP requests.

Revocation, Suspension and Un-suspension

See procedure for Locally stored BankID in the section 7.2.