

RA move and merger template

| | |
|---|--|
| Ceremony description | RA Ceremony (Key Change Over) RA Merger RA Move |
| Date and time for the ceremony | |
| Status for the ceremony | PLANNING |
| Date and time for the activation, switchover and revoke | |
| Status for the activation, switchover and revoke | PLANNING |
| References | |

Resources bank and TSP:

| Role | Name | Contact information |
|---------------|------|---------------------|
| Key custodian | | |
| Other | | |

Resources BankID:


| Role | Name | Contact information |
|-------------|------|---------------------|
| Coordinator | | |
| PKI | | |
| App | | |

Definitions:

| What | Description |
|------------|---|
| Ceremony | The physical meeting with all necessary participants. This is when the new RA certificate is created in red zone. |
| Activation | When the new certificate is activated on BankID side. This is usually done at another time than the ceremony. |
| Switchover | When the traffic is switched from the old CA to the new CA. This is usually done within 24 hours from the activation, but can also be done separately. |

Before the ceremony:

| Step | Description | Responsible | Task | Deadline | Status | Documents and notes |
|------|-------------|-------------|------|----------|--------|---------------------|
|------|-------------|-------------|------|----------|--------|---------------------|

| | | | | | | |
|-------------------------------|---|-------------|--|--|----------|---|
| 1) Set up internal routines | The respective TSP or Bank will require to have in place internal routines for move or merger of RA's. | TSP or Bank | <p>Decide the following:</p> <ul style="list-style-type: none"> How to deal with the OTP tokens End user impact Information to end users How to deal with logs and how/who to archive (admin logs for certificates) <p>Note that the TSP/Bank is responsible for handling the end user certificates through the whole process, including revoke of old certificates.</p> | | PLANNING | |
| 2) BITS Approval | The respective TSP or Bank will require BITS approval for the following move or merger before ordering an RA ceremony. | TSP or Bank | <ul style="list-style-type: none"> The TSP/Bank describes the change Send email to Lise. Arneberg@bits.no and Torgeir. Sorvik@bits.no for approval | | PLANNING | <p>Information from BITS about the process:</p>  |
| 3) Formal order to BankID | The respective TSP or Bank have to create and send a formal order to BankID as an electronically signed document, signed by TSP or Bank. | TSP or Bank | <p>This order should contain:</p> <p>New RA:</p> <ul style="list-style-type: none"> Detailed information about the CA Approval from BITS (from step 2) <p>Move or merger of RA:</p> <ul style="list-style-type: none"> The purpose of the move or merger of the mentioned RA Detailed move or merger from and to what CA Approval from BITS (from step 2) <p>Sign it electronically and create a ticket here with the signed document attached.</p> | | PLANNING | |
| 4) Send order forms to BankID | <p>The respective TSP or Bank have to fill out required order forms and send it to BankID signed before or during the RA ceremony.</p> <p>A copy must be sent before the RA ceremony.</p> | TSP or Bank | <ul style="list-style-type: none"> TSP/Bank fills out the required order form. Send a copy before the RA ceremony by creating a ticket here. | | PLANNING | Order form templates can be found here: Misc forms for BankID Support |

| | | | | | | |
|--|--|-----------------------|---|--|----------|--|
| 5) Make sure that the prerequisites are in order | <p>Primary CAO token "Dongle" is normally stored in a safe at the respective TSP (CA responsible).</p> <p>The respective Key Custodian for the TSP is responsible to carry and bring the RA XML request and the Primary CAO token "dongle" to the RA ceremony.</p> | Key custodian for TSP | <ul style="list-style-type: none"> • Create an RA XML request on the TSP system, for example through HAT tool. • Make sure that the USB stick is new and unused • Make sure that the Key Custodian have approved identification such as a passport or driver license (if the Key Custodian is a non-Norwegian citizen, they must bring their passport) | | PLANNING | |
| 6) RA ceremony coordination | BankID will ensure that everything is in place and coordinate the ceremony and switchover with all stakeholders. | BankID | <p>Check that the following is in place:</p> <ul style="list-style-type: none"> <input type="checkbox"/> BITS approval - If not provided by the TSP or Bank, contact BITS and verify <input type="checkbox"/> Formal order received <input type="checkbox"/> Signed order forms <ul style="list-style-type: none"> <input type="checkbox"/> Signed - Naming of RA (Required) <input type="checkbox"/> Signed - Revoke RA XML Request (Optional) <input type="checkbox"/> TSPs Primary CAO token <input type="checkbox"/> TSPs/Bank RA XML Request <p>If all is in place, all stakeholders align and agree on date and time for the following:</p> <ul style="list-style-type: none"> <input type="checkbox"/> 1. RA ceremony <input type="checkbox"/> 2. Activation of New RA XML Sign Certificate <input type="checkbox"/> 3. Switchover <input type="checkbox"/> 4. Revoke RA XML (Optional) <p>Normally step 2, 3 and 4 happens within the same 24h.</p> | | PLANNING | |
| 7) Invitations | BankID will send out a meeting invite for the ceremony and the switchover. | BankID | <p>Create and send out the invitation to all stakeholders.</p> <p>The invitation should contain, but not limited to:</p> <ul style="list-style-type: none"> • Purpose and description • Date • Time • Duration • Virtual Meeting Link or Address • Attendees and contact points • Information on what to bring | | PLANNING | |

Ceremony:

The Key Custodian for the respective TSPs is on-site with their Primary CAO token and the RA XML sign request.

| Step | Description | Responsible | Task | Deadline | Status | Documents and notes |
|--------------------------|--|-------------|--|----------|----------|---------------------|
| 8) Pre RA ceremony check | BankID will greet the participants and check that all is OK for moving on with the ceremony. | BankID | <ul style="list-style-type: none"> Participants need to sign in and out All necessary resources are in place <ul style="list-style-type: none"> Key Custodian PKI App Key Custodian ID check is done by the SO USB virus scan is done manually before High secure room (USB stick that contains the RA XML Sign request) All required documentation is in place <ul style="list-style-type: none"> Note that RA naming order forms are to be stored in the BankID High secure room. When the documentation is signed electronically, a copy of the document is to be stored | | PLANNING | |
| 9) Perform RA ceremony | BankID is to perform the RA ceremony | BankID | <p>BankID will guide the key custodian through issuing of the new RA XML/SSL certificate(s) on the new CA.</p> <p>Key custodian will need to oversee that the changes made are according to the documentation.</p> | | PLANNING | |

After the ceremony:

| Step | Description | Responsible | Task | Deadline | Status | Documents and notes |
|--|---|--------------|--|----------|----------|---------------------|
| 10) Request activation | TSP/Bank need to send a request to BankID | TSP and Bank | <ul style="list-style-type: none"> Write a request for activation of New RA XML Sign certificate(s) in BankID. The request needs to contain the following: <ul style="list-style-type: none"> Time for the activation Which originator(s) to activate Which CA it concerns Create a ticket here | | PLANNING | |
| 11) Activation and switchover coordination | BankID will coordinate the switchover with all stakeholders. | BankID | <p>BankID will coordinate with the required resources.</p> <p>If not already set, agree on the date and time for:</p> <ul style="list-style-type: none"> <input type="checkbox"/> 1. Activation of New RA XML Sign Certificate <input type="checkbox"/> 2. Switchover <input type="checkbox"/> 3. Revoke RA XML (Optional) <p>Normally happens within the same 24h.</p> | | PLANNING | |
| 12) Activation | BankID is to activate the new certificates. This is normally done during the same day as the Switchover. | BankID | <p>Activate the new RA XML Sign certificate(s) in BankID.</p> <p>Performed by AO with PKI involved.</p> | | PLANNING | |
| 13) Certificate check | Check that the certificate is working | TSP and Bank | <p>TSP/Bank needs to check that the new activated certificate is working towards ODS.</p> <p>Check that the new certificate have access to display the existing certificates on the old CA.</p> | | PLANNING | |

| | | | | | | |
|---------------------------|--|----------------------|---|--|----------|---|
| 14) Switchover and revoke | Plan and implement the switchover and revoke. | TSP, Bank and BankID | <ol style="list-style-type: none"> 1. TSP/Bank: Write a request for switchover issuing CA in BankID from old to New CA. Include the time wanted for this. Create a ticket here 2. BankID: <ol style="list-style-type: none"> a. Do the switchover b. Those who perform the switchover will inform the TSP /Bank by phone when it has been done 3. TSP/Bank: Run test case sets to verify <ol style="list-style-type: none"> a. TSP/Bank: If successful, move to the next step b. BankID: If unsuccessful, investigate and resolve then move to next step c. BankID: if unsuccessful, not possible to fix, do a rollback <ul style="list-style-type: none"> • Bank/TSP: When rollback is done, run test case sets to verify 4. (optional. If not done, the certificate will be active on the old CA until it expires) Bank/TSP: Send an order for revoke of old RA XML Sign certificate in BankID by creating a ticket here 5. (optional) BankID: Revoke the old certificate | | PLANNING | Order form templates can be found here: Misc forms for BankID Support |
| 15) Renewals | Renewals of end users, merchants etc. As decided in step 1. | TSP and Bank | <ol style="list-style-type: none"> 1. Bank renew end user BankID certificates 2. Bank asks merchants to renew merchant BankID's using HAT 3. Possible change of OTP Service by adding a new and then removing the old <p>This is best done outside of peak hours to reduce the risk of latencies.</p> | | PLANNING | |