LØSNINGSBESKRIVELSE

BUYPASS ACCESS SOLUTION

Buypass Bedriftsløsning - LRA-klient .net versjon

ÅPEN

Dokumentversjon: 4.2
Versjonsdato: 05.10.2014

Buypass AS
Nydalsveien 30A, PO Box 4364 Nydalen
N-0402 Oslo, Norway
Tel.: +47 23 14 59 00
Fax: +47 23 14 59 01
E-mail: kundeservice@buypass.no
VAT: NO 983 163 327
www.buypass.no

Endringshistorie

Versjon	Dato	Status	Beskrivelse/Endringer
1.0	13.10.2011	Versjon	Gjennomgang og oppdatering for LRA v2.1.
1.1	31.01.2012	Versjon	Oppdatering for LRA v 2.5 og distribuerte funksjoner.
2.0	19.07.2012	Versjon	Oppdatering basert på koordinering med annen LRA-dokumentasjon.
2.1	19.11.2012	Versjon	Oppdatering dokumentliste.
3.0	19.08.2013	Versjon	Oppdatering basert på nye releaser 2013 og koordinering med annen LRA-dokumentasjon.
4.0	16.01.2014	Versjon	Oppdatering for ny .net versjon av LRA-klienten (v3.1)
4.1	18.05.2014	Intern versjon	Oppdatering for ny .net versjon av LRA-klienten (v3.2)
4.2	05.10.2014	Versjon	Justeringer og tilpasninger for .net versjon og publisering på Buypass Dokumentsenter

Dokumentets plassering og navn:
T:\Produkt\Utvikling\Produkt\LRA\Dokumentasjon\Dok 00 - Løsningsbeskrivelse\Gjeldende versjon\LRA klient v3_Løsningsbeskrivelse bedriftsløsninger_v4.2.docx

Innholdsfortegnelse

1 Begreper og definisjoner

Begrep	Forkortelse	Beskrivelse
Active Directory	AD	Katalogtjeneste som inneholder informasjon om bruker og gir tilganger og rettigheter.
BEID		Benevnelse på en sertifikatapplikasjon som ligger i chipen på et smartkort, og som kan inneholde alle typene av sertifikater.
Bruker		Person som er ansatt eller innleid i bedriften.
Buypass	BP	Buypass AS – leverandør av Bedriftsløsningen LRA og kvalifiserte sertifikater til brukere (PKI).
Buypass systemer	BPS	Fellesbenevnelse på alle systemer som utvikles og forvaltes av Buypass.
Certificate Authority	CA	System for utstedelse og vedlikehold av sertifikater.
Certificate Revocation List	CRL	Oversikt over sperrede sertifikater.
Det Sentrale Folkeregisteret	DSF	Et offentlig register over alle personer som bor eller har vært bosatt i Norge.
Distribuert LRA	DLRA	Funksjonalitet i LRA-klient for fjernbehandling av sertifikater; registrering, utstedelse og vedlikehold. Det vil si behandling av sertifikater for brukere som befinner seg på lokasjoner utenfor sentralt ID-kontor.
Dokumentregister		Register hvor dokumenter fra legitimasjonskontroll og operasjoner for utstedelse og vedlikehold av sertifikater lagres – kontrolldokumenter.
Enrollment Agent sertifikat	EA	Sertifikat som kun benyttes internt i bedriften. Sertifikatet benyttes av RA-ADMIN og Operatører ved utstedelse og vedlikehold av brukernes sertifikater gjennom LRA-klienten.
ID-kontor		Kontor/lokasjon hvor brukerne henvender seg for utstedelse og administrasjon av ID-kort/ansattkort med visuell identifikasjon og fysisk adgangskontroll i tillegg til sertifikater.
ID-kort		Se smartkort.
Kontrolldokument	PDF	Signert dokument (pdf) som inneholder informasjon knyttet til gjennomført kontroll ved operasjoner for utstedelse og vedlikehold av sertifikater. Kontrolldokumentene lagres i Dokumentregisteret.
Kortleser		Periferutstyr til LRA-PC hvor Operatører og brukere setter inn smartkortet sitt.
Kvalifiserte sertifikater	QC	Sertifikater som benyttes til identifisering og signering også utenfor bedriften. Sertifikatutsteder av kvalifiserte sertifikater er Buypass.
Local Registration Authority	LRA	Autorisasjon for lokal registrering, utstedelse og vedlikehold av sertifikater.
Lokalt sertifikat	LC	Sertifikat som kun benyttes internt i bedriften. Sertifikatet benyttes til pålogging av PC-er og adgang til systemer.
LRA-klient		Applikasjon for behandling av sertifikater; registrering, utstedelse og vedlikehold – se Local Registration Authority (LRA).
LRA Operatør		Person som sammen med RA-ADMIN er ansvarlig for behandling av sertifikater på ID-kontoret ved hjelp av LRA-klienten.
LRA PC		PC som er en dedikert LRA-klient eller LRA Satellite

Begrep	Forkortelse	Beskrivelse
LRA Satellite		LRA-klient med begrenset funksjonalitet.
LRA Satellite Operatør		Person som er ansvarlig for behandling av sertifikater på LRA Satellite.
Operatører		Fellesbenevnelse for RA-ADMINer , LRA Operatører og LRA Satellite Operatører.
PIN tastatur	PIN PAD	Periferutstyr til LRA-PC hvor brukeren taster PIN.
RA-ADMIN		Person som er ansvarlig for å opprette LRA Operatører samt behandling av sertifikater på lik linje som LRA Operatører.
Remote Server Administration Tools	RSAT	MicroSofts administrasjonspakke
Signaturplate		Periferutstyr til LRA-PC hvor bruker kan skrive signaturen sin.
Smartkort	ID-kort	Smartkort til brukere i bedriften. Kortet gir brukeren adgang til lokaler og tilgang til PC-er og systemer.
Skanner		Periferutstyr til LRA-PC hvor legitimasjon kan skannes inn.
Tredjepart		Person som er ansatt i bedriften og som kjenner/kan gå god for øvrige personer i bedriften ved legitimasjonskontroll.

2 Innledning

Buypass Access Solution inngår i **Buypass Bedriftsløsning**. Det er en løsning for effektiv og sikker tilgang til virksomhetens interne og eksterne tjenester som krever elektronisk ID for identifisering, signering og kryptering. Løsningen inkluderer eget administrasjonsgrensesnitt for lokal utstedelse av smartkort med elektronisk ID på ulike sikkerhetsnivå, og kan inkludere fysisk adgangskontroll i samme kort.

Løsningen støtter bruk av **bedriftens egne sertifikater** for tilgang til nettverk og andre lokale tjenester, samt **Buypass kvalifiserte sertifikater** som blant annet brukes for meldingsutveksling og tilgang til en rekke offentlige tjenester – i ett og samme kort.

Buypass Access Solution består av følgende komponenter:

- **Buypass Access Manager** - Local Registration Authority (LRA). Et administrasjons-system for utstedelse og administrasjon av både *lokale sertifikater* fra lokal Microsoft CA og *kvalifiserte sertifikater* (PKI nivå4) fra Buypass CA
- **Buypass Smartkort** - kort med chip som kan inneholde begge typer sertifikater i tillegg til fysiske egenskaper som magnetstripe og RFID
- **Buypass Access Enterprice** - klientprogramvare for installasjon på den enkeltes PC eller på terminalserver. Programvaren sørger for kommunikasjon med programmer som skal ha tilgang til å benytte sertifikatene på smartkortet

Denne løsningsbeskrivelsen gir oversikt over hva som skal til for å integrere Buypass Access Solution og LRA i bedriftens infrastruktur. Tilpasningsbehov og forutsetninger for infrastruktur beskrives.

De 3 første kapitlene er sammenfallende med tilsvarende kapitler i dokumentet **System- og teknisk guide for Buypass Access Solution**.

2.1 Egnethet

Buypass Bedriftsløsninger passer best for bedrifter som har ønske om å utstede sertifikater selv eller evt. via tredjepart. Gjerne i kombinasjon med visualisering (bilde og signatur) og fysisk adgangskontroll (magnetstripe/RFID/strekkode).

2.2 Bruksområde

Smartkort med sertifikater kan blant annet ha følgende bruksområder:

- Sikker pålogging til bedriftens IT-systemer og ressurser fra intern arbeidsplass (MS Smartcard logon / Terminalserver)
- Sikker pålogging til bedriftens IT-systemer og interne ressurser fra fjernarbeidsplass (VPN)
- Single Sign On (SSO)
- Signering og kryptering i fagsystemer med kvalifiserte sertifikater (Buypass kvalifiserte sertifikater)
- Signering og kryptering av dokumenter og e-post (Microsoft Outlook) med kvalifiserte sertifikater
- Identifisering, signering og kryptering med kvalifiserte sertifikater i bedriftens 3. parts programvare
- Tilgang til offentlige tjenester med kvalifisert sertifikater som AltInn, NAV m.m.

2.3 Kvalifiserte sertifikater - PKI

Buypass er registrert hos Post- og teletilsynet som utsteder av kvalifiserte sertifikater i henhold til Lov om e-signatur. LOV 2001-06-15-81: Lov om elektronisk signatur og FOR-2001-06-15-611: Forskrift om krav til utsteder av kvalifiserte elektroniske sertifikater. Buypass kvalifiserte sertifikater er deklarert i henhold til Selvdeklarasjonsforskriften og tilfredsstiller Kravspesifikasjon for PKI i offentlig sektor, versjon 2.0, fra 2012.

Buypass arbeider etter nasjonale og internasjonale standarder for å tilfredsstille beste praksis på området. Buypass kvalifiserte sertifikater er i henhold til "SEID – Anbefalte sertifikatprofiler for personsertifikater og Virksomhetssertifikater, versjon 1.02" (tilgjengelig på www.npt.no). Buypass kvalifiserte sertifikater utstedes av Buypass Class 3 CA.

2.3.1 Buypass RA - delegering av ansvar

Buypass er utsteder av og sertifikatautoritet for Buypass kvalifiserte elektroniske sertifikater, regulert i LOV 2001-06-15-81: Lov om elektronisk signatur og FOR-2001-06-15-611: Forskrift om krav til utsteder av kvalifiserte elektroniske sertifikater.

Bedrifter som skal benytte Buypass kvalifiserte sertifikater må inngå en avtale med Buypass hvor Buypass delegerer myndighet til å utstede og administrere kvalifiserte sertifikater på vegne av Buypass. Bedriften blir registrert som en Buypass RA (Registration Authority). Bedriften godtar ved inngåelse av avtalen Buypass' krav og retningslinjer for utstedelse av kvalifiserte sertifikater. I den forbindelse utnevner bedriften et antall personer (minimum 2 personer) som RA-ADMINer (Registration Authority Administrator). RA-ADMIN får rettigheter til å delegere ansvaret videre internt i bedriften til LRA Operatører.

Ansvar og plikter for involverte parter/personell er beskrevet i Certificate Policy (CP) for Buypass Class 3 Certificates. Se http://www.buypass.no/kundeservice/nedlastingssenter under overskriften CA Dokumentasjon (juridisk).

2.4 Brukere av løsningen

Det vil kun være autoriserte Operatører som kan betjene Buypass Access Manager - LRA-klienten. Operatører er fellesbenevnelse på RA-ADMINer og LRA Operatører. Begge er roller som har ansvaret for utstedelse og administrasjon av sertifikater til brukere / ansatte. Rollene benevnes som Operatører i fortsettelsen med mindre funksjoner er forbeholdt en av rollene.

2.5 Relevante dokumenter

- Løsningsbeskrivelse for LRA Buypass Bedriftsløsning (dette dokumentet)
- Buypass Access Enterprise - bestillingsformular for spesialtilpasninger CSP (gjennomgås sammen med Buypass teknisk konsulent)
- MS Windows2008 CA_AD_CRL Buypass / MS Windows2012R2 CA_AD_CRL Buypass
- MS CA Certificate Templates Buypass
- MS AD Certificate Groups Buypass
- LRA client Readme – installasjonsguide og release-beskrivelse
- Configuration Application LRA client – guide for konfigurering av LRA-klienten
- System- og teknisk guide Buypass Access Solution (JAVA og .net)
- Brukerveiledning og rutiner for Buypass Access Solution
- Abonnementsavtale for Brukerstedssertifikat

- Avtale om utstedelse og administrasjon av Buypass kvalifiserte sertifikater med fullmaktskjema (RA-avtale)
- Instruks for RA-ADMIN og LRA Operatører
- Ansattkort – tips til informasjon
- Avtalevilkår Buypass kvalifiserte sertifikater (Kundeavtale) – finnes på Buypass nettside under Nedlastingssenteret, fanen CA Dokumentasjon (juridisk) og Personlige kvalifiserte sertifikater.

Det meste av dokumentasjon er tilgjengelig på Buypass Dokumentsenter – se Buypass Access Solution.

3 Buypass Access Solution – systembeskrivelse

Utgangspunktet for en bedriftsløsning er at smartkort med sertifikater skal benyttes for å logge seg på, gjennomføre elektronisk signeringer og eventuelt kryptering i bedriftens IT-systemer – interne og eksterne. For at smartkort skal fungere må eksisterende infrastruktur være oppdatert med følgende komponenter:

- **Buypass Access Manager** - LRA-klient – programvare som utsteder og administrerer sertifikater for bedriftens brukere fra lokal CA og Buypass CA

- **Smartkort** med Buypass chip som kan inneholde kombinasjonen av lokale og kvalifiserte sertifikater

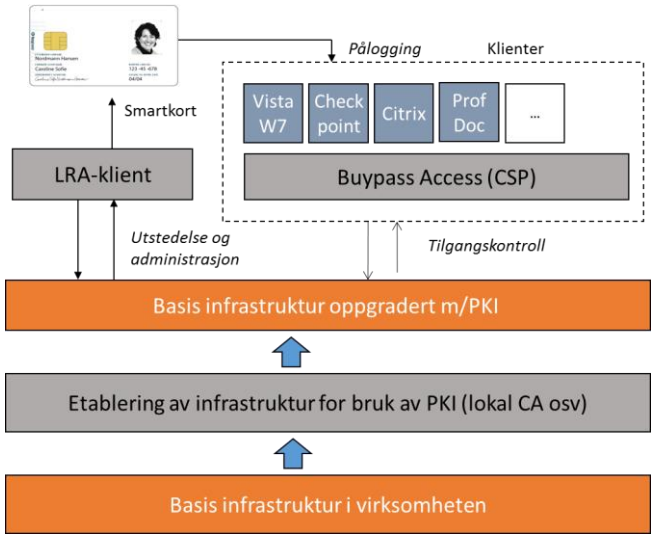
- **Lokal MS CA** (Microsoft Certificate Authority) med tilhørende CRL (Certificate Revocation List)
  - Lokal CA utsteder lokale sertifikater som kan benyttes internt i bedriften
  - CRL er en liste over sperrede lokale sertifikater
  - Alle PCer og terminaler må ha tilgang til CRL

- **Lokal MS AD** (Microsoft Active Directory) for administrasjon av bedriftens brukere

- Åpning mot **Buypass CA** med tilhørende CRLer (Certificate Revocation List)
  - Buypass CA utsteder kvalifiserte sertifikater som kan benyttes internt i bedriften eller eksternt mot lukkede fagsystemer eller åpne tjenester
  - CRL er en liste over sperrede kvalifiserte sertifikater

- **Buypass Access Enterprice** – programvare som kommuniserer med smartkortet. Programvaren installeres på PCer, terminalservere og eventuelt andre servere hvor smartkort skal benyttes. Programvaren omtales også som en CSP (Certificate Service Provider)

- PC-er og/eller terminaler må ha tilkoblet **kortleser for smartkort**

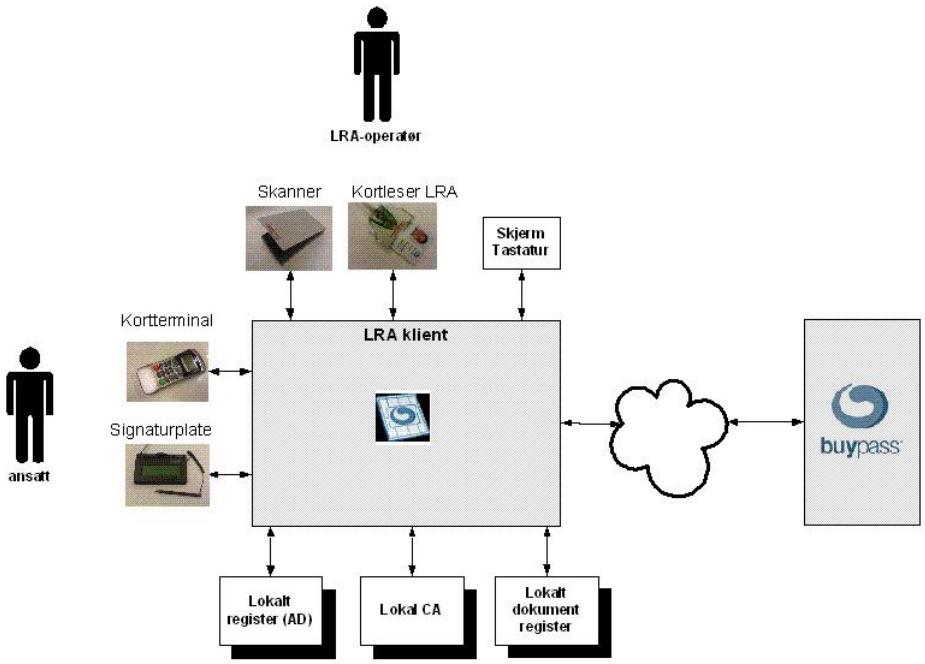


Figur: Overordnet illustrasjon av hvordan Buypass Access Solution integreres med eksisterende infrastruktur hos bedriften.

3.1 Buypass Access Manager – LRA-klienten

Buypass Access Manager – LRA-klienten installeres på en PC (LRA-PC) som befinner seg på egnet området hindret for innsyn direkte på skjermen på grunn av tilgang til brukerinformasjon. Buypass har ingen eksplisitte krav til LRA-PC, men anbefaler bruk a stasjonær maskin eller en bærbar PC med litt størrelse på skjerm og stor strømkapasitet for tilkobling av periferiutstyr.

Buypass Access Manager er en klientapplikasjon, kjent som LRA-klienten, som benyttes for utstedelse og administrasjon av lokale påloggingssertifikater og kvalifiserte sertifikater fra Buypass. Sertifikatene utstedes til brukere / ansatte hos Brukerstedet, og lastes ned i Buypass chip på ID-kortene.



Figur: Skisse over LRA-klienten med alle eksterne enheter og eksterne systemer som er involvert.

LRA-klienten betjenes av en **Operatør** som selv benytter sitt personlige ID-kort for autentisering og elektronisk signering. I forbindelse med utstedelse av sertifikater skal det gjennomføres en legitimasjonskontroll som inkluderer innskanning av legitimasjonsdokument og innhenting av ansattes håndskrevne signatur.

LRA-klienten henter opplysninger om ansatte som skal ha sertifikater fra et lokalt **Microsoft Active Directory (AD)**. De lokale sertifikatene utstedes fra en lokal **Microsoft Certificate Authority (CA)**.

Lokalt dokument register, er et område i nettverket med begrenset tilgang, hvor alle kontroll-dokumenter (PDFer) fra LRA-klienten lagres. De fleste operasjoner som utføres i LRA-klienten blir dokumentert i form av kontrolldokumenter. Operatøren bekrefter operasjonene gjennom å signere disse dokumentene elektronisk. For operasjoner som også inkluderer kvalifiserte sertifikater vil en kopi av kontrolldokumentet bli oversendt Buypass.

LRA-klienten kommuniserer med ***Buypass sentrale systemer*** **(BPS)** via et eget grensesnitt (**LTS/WebLTS**) hvor alle meldinger signeres og krypteres. Dette benyttes ved pålogging på LRA-klienten og i forbindelse med operasjoner som involverer kvalifiserte sertifikater. Hvis Buypass ikke er tilgjengelig, vil LRA-klienten operere i lokal modus og kun utstede og administrere lokale sertifikater.

3.2 Smartkort

Et ID-kort er et Buypass smartkort. Smartkortet har en chip med Multos operativsystem og en elektronisk ID-applikasjon som kan inneholde flere sertifikattyper, både lokale og kvalifiserte. Bedriften avgjør i hvert enkelt tilfelle hvilke sertifikater en bruker skal ha.

Fysiske tilganger og utseende på smartkortet er ikke en del av Buypass Bedriftsløsninger, men ivaretas av bedriften internt eller av en annen aktør.

1. Visuell identifikasjon (bilde, signatur og ansattnummer)
2. Strekkode – tidsregistrering
3. Magnetstripe – adgangs-kontroll, betaling, etc.
4. Berøringsfri teknologi (MIFARE, HID m.fl) – adgangskontroll, biometri, betaling, etc.
5. Buypass chip – lagring av sertifikater (lokale og/eller kvalifiserte)
6. Buypass hologram – akseptansemerke og et ikke kopierbart sikkerhetselement

Figur: Smartkort og mulig innhold

3.3 Microsoft CA og AD

Lokale sertifikater utstedes via **Microsoft Certificate Authority (CA)**. Lokale sertifikater kan være sertifikater beregnet for brukere (brukersertifikater) eller for klienter/pc/servere/andre fysiske enheter (maskinsertifikater). LRA-klienten administrerer lokale brukersertifikater.

En CA forutsetter tett integrasjon med **Microsoft Active Directory (AD)** som administrerer brukerne av sertifikatene. Det er en en-til-en kobling mellom CA og AD. Installasjon av lokal CA medfører at det også må opprettes brukere og grupper i lokal AD.

En lokal CA åpner for at bedriften selv kan sette varigheten på sertifikatene. Det er også mulig å definere forskjellige sertifikattyper med ulike varighet. Dette gir for eksempel bedriften mulighet til å utstede lånekort med kun få dagers/timers varighet.

Ved etablering av en lokal CA kan bedriften velge å utarbeide en **Certificate Policy (CP)** samt en **Certificate Practice Statement (CPS)**. En **CP** inneholder et sett med regler som sier hvordan sertifikatene utstedes og behandles, mens en **CPS** beskriver hvordan reglene i CPen etterleves. Dette er ikke et krav – mange støtter seg til **Buypass Certificate Policy for Buypass Class3 Qualified Certificates** som finnes på Buypass Nedlastingssenter under fanen CA Dokumentasjon (juridisk) og Personlige kvalifiserte sertifikater.

Lokal CA kan og bør inkluderes i et CA hierarki i form av rotsignering. Det åpner for tillit mellom bedrifter i samme CA hierarki. Sikkerhetsmessig bør **rotCA være offline**, mens underliggende utstedende CAer er online. Når lokal CA inngår i et hierarki skal rot CAens CP aksepteres. Hvordan bedriften etterlever rot CAens CP, kan dokumenteres for eksempel i en CPS.

MS CA er en del av MS Windows Server (forutsetter en Enterprise versjon.

3.3.1 CRL

MS CA produserer jevnlig lister over sperrede sertifikater også kalt sperrelister eller CRLer. Sperrelistene har en varighet som settes av bedriften. Sperrelisten må publiseres på en, men gjerne flere kilder (AD, http, fil). Lenke(r) legges inn som informasjonselement i sertifikatene.

Alle arbeidsstasjoner, terminalservere og lignende som benyttes til pålogging må ha tilgang til sperrelisten. I de tilfeller hvor sperrelisten er utilgjengelig eller gått ut på dato vil pålogging ikke være mulig. Det er kritisk for bedriften at en gyldig sperreliste er tilgjengelig til enhver tid. Sperrelisten bør derfor være redundant.

3.4 Buypass Access Enterprice – CSP

Klientprogramvaren Buypass Access benyttes for kommunikasjon med smartkortet og må installeres på bedriftens arbeidsstasjoner og/eller terminalservere.

Buypass Access omtales også som en **CSP (Certificate Service Provider)**. Enterprice-versjon gir bedriftsspesifikt oppsett i forhold til bedriftens infrastruktur. Eget skjema fylles ut for foretaksspesifikke tilpasninger. Dette gjøres sammen med teknisk konsulent fra Buypass før oppstart.

4 Buypass Access Manager – systembeskrivelse

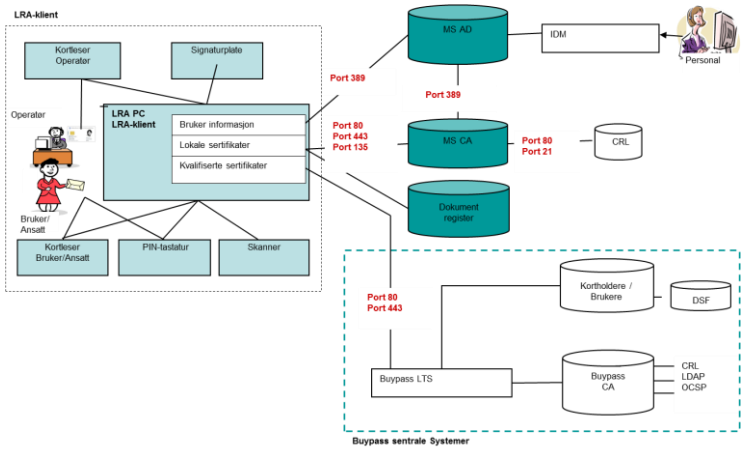
4.1 Programvare og annet utstyr

Buypass Access Manager er klientprogramvare som er utviklet av Buypass. Tidligere var den kjent som **Buypass LRA (Local Registry Authority)**, men i 2014 fikk den navnet **Buypass Access Manager** som en del av **Buypass Bedriftsløsning** – **Buypass Access Solution**.

Nyeste versjon av klienten er utviklet i .NET. Programvaren må installeres på en egen PC (**LRA-PC**).

LRA har følgende nheter/komponenter/grensesnitt:

- LRA-PC
- Kortlesere for Operatørkort og Brukerkort
- PinPad hvor Bruker setter PIN på eget smartkort
- SignaturPad hvor Bruker signerer og aksepterer vilkår for utstedelse
- Skanner hvor Brukers legitimasjonsdokument skannes ved førstegangsutstedelse av sertifikater
- Lokal MS CA/AD
- Buypass sentrale systemer (BPS)
- Lokale filområder for PDF-filer, rapporter og fjernadministrasjon



Figur: LRA med tilhørende periferutstyr, beskrivelse av porter og grensesnitt. Illustrerer hvilke systemer som involveres ved utstedelse og administrasjon av både lokale og kvalifiserte sertifikater.

LRA må ha følgende portåpninger:

- AD – Port 389 (LDAP)
- CA – Port 80, 443 og 135 (RPC)
- Lokalt dokument register – 135,137 og 139 (filoverføring til filområde)
- BPS – Port 80, 443 – kommunikasjon over https. Krav til åpninger i brannmur mot adressene:
  - **.NET-versjon**
    - PROD: https://www.buypass.no/weblts/p1
    - TEST: https://www.test4.buypass.no/weblts/p1
  - **JAVA-versjon**
    - PROD: https://www.buypass.no/lts/service
    - TEST: https://www.test4.buypass.no/lts/service

  NOTE: Om et Brukersted setter opp sin infrastruktur mot både TEST og PROD avklares under implementering.

4.2 Funksjoner

Buypass Access Manager – LRA er klientprogramvare for utstedelse og administrasjon av lokale sertifikater (intern MS CA) og/eller kvalifisert sertifikater (Buypass CA for kvalifiserte sertifikater).

LRA-klienten støtter følgende funksjoner:

- Utstede nye ID-kort med lokale og/eller kvalifiserte sertifikater
- Utstede erstatningskort med lokale og/eller kvalifiserte sertifikater
- Fornyelse av lokale og/eller kvalifiserte sertifikater
- Utstede lånekort med lokale sertifikater med kortere levetid
- Sperring av kort og sertifikater
- PIN-kode administrasjon – avblokkering av sperret PIN / endre PIN
- Fjernfunksjoner for sertifikater fra lokal Microsoft CA *)
- Smartkortdiagnose – feilsøking
- Opprette og administrer Operatører og sertifikater for Operatører
- Rapporter:
    1. Oversikt over sertifikater utstedt til angitt person
    2. Oversikt over sertifikater utstedt i en angitt periode
    3. Oversikt over sertifikater som utløper i en angitt periode
    4. Oversikt over utstedte midlertidige kort - lånekort

) Fjernfunksjoner – distribuert LRA

LRA-klienten har, sammen med Buypass Access Enterprise, funksjonalitet for fjernbehandling av sertifikater fra lokal MS CA; registrering, utstedelse og vedlikehold. Det vil si behandling av sertifikater for brukere som befinner seg på lokasjoner utenfor sentralt ID-kontor.

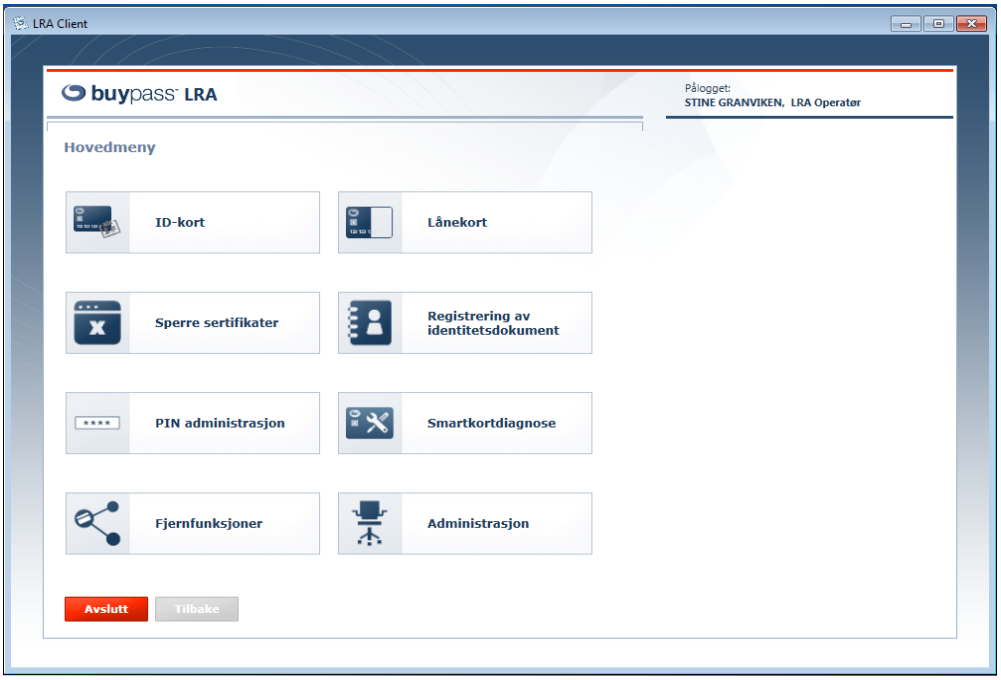
Brukeren må ha kontakt med sentralt ID-kontor og en LRA Operatør via telefon for å få utført ønsket operasjon, men det gir samtidig brukeren mulighet til å administrere smartkortet sitt fra egen PC.

Distribuert LRA støtter følgende funksjoner:

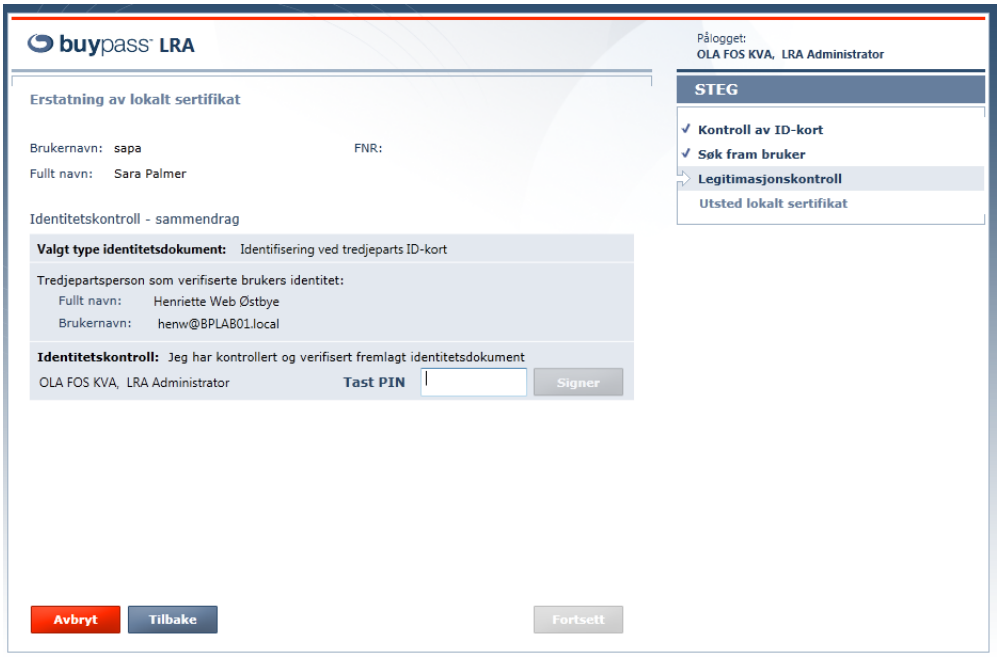
- Aktivering av nytt ID-kort (ID-kort er utstedt sentralt)
- Fornyelse av lokalt brukersertifikat på smartkort
- Utstedelse av lånekort
- Avblokkering av PIN

NB! Fjernfunksjoner gjelder pt. kun administrering av lokale sertifikater fra lokal MS CA.

4.3 Menyer - skjermbilder



Figur: Hovedmenyen i LRA-klienten.



Figur: Utstedelse av ID-kort – et eksempel på prosesstyrt operasjon med veiledning for Operatør.

4.4 Konfigurering

Gjennom oppsett av LRA er det mulig å bestemme hvilke funksjoner en LRA skal settes opp med - om det er en fullstendig installasjon med alle funksjoner, eller om det er en begrenset installasjon med kun et fåtall funksjoner. Ved installasjon er det altså mulig å skreddersy en klient til å inneholde kun de funksjoner som er nødvendig. Her er noen eksempler:

- LRA-klienten på ID-kontoret vil være en fullstendig klient med ALLE funksjoner

- LRA-klienten på Kundesupport vil være en begrenset klient med kun PIN-administrasjon
- LRA-klienten på Personalkontoret eller IKT-kontoret vil være en begrenset klient med kun Preregistrering av brukere

4.5 LRA Modes

Buypass Access Manager - LRA-klienten kan settes opp og konfigureres i 3 ulike modus for å tilpasse bedriftens behov. For de ulike modusene vil det være behov for ulik oppkobling av de eksterne grensesnittene.

1. **Local Mode**: Utstedelse og vedlikehold av kun lokale sertifikater (MS CA). Her er det ingen kommunikasjon mot Buypass. Brukere og sertifikatgrupper sjekkes kun mot lokal AD

2. **Buypass Mode**: Utstedelse og vedlikehold av kun kvalifiserte sertifikater (Buypass CA). Her er det kun kommunikasjon mot Buypass, og ingen avsjekk mot lokal AD. Brukerne registreres og vedlikeholdes kun hos Buypass (Customer Management System)

3. **Mixed Mode**: Utstedelse og vedlikehold av både lokale og kvalifiserte sertifikater. Her er det både kommunikasjon mot lokal AD og mot Buypass. Brukere og sertifikatgrupper sjekkes mot lokal AD, og i tillegg må brukere som skal ha kvalifiserte sertifikater være registrert hos Buypass

5 Sertifikatbehov

For bedrifter som har behov for sertifikater som skal benyttes både internt i bedriften i tillegg til sikker identifisering, signering og kryptering utenfor bedriften må det utstedes kvalifiserte sertifikater fra Buypass i tillegg til lokale sertifikater fra bedriften.

Bruksområde
Kvalifiserte sertifikater benyttes for å oppnå:

- Signering og kryptering i fagsystemer med kvalifiserte sertifikater (Buypass sertifikater)
- Signering og kryptering av dokumenter og Microsoft Outlook med kvalifiserte sertifikater.
- Identifisering, signering og kryptering med kvalifiserte sertifikater i bedriftens 3. parts programvare.
- Tilgang til offentlige tjenester med kvalifisert sertifikater som for eksempel AltInn, NAV m.m.

I tabellen nedenfor er behovet for de ulike komponentene oppsummert avhengig av type sertifikater som bedriften ønsker. Aktuelle sertifikat kombinasjoner er:

L 1 - Lokale sertifikater
L 2 - Lokale og kvalifiserte sertifikater
L 3 - Kvalifiserte sertifikater

Komponenter	L1	L2	L3	Inneholder	Kommentar
Lokal MS CA & AD	√	√		Lokal MS CA utsteder og administrer lokale sertifikater. MS CA forutsetter integrasjon med MS AD. MS CA produserer lister over sperrede sertifikater (CRL). CRLene legges på en web server som må være tilgjengelig fra alle arbeidsstasjonene tilknyttet bedriftens domene.	MS CA inngår i MS Server 2003 / 2008 Enterprise / 2008 Standard R2.
Buypass CA		√	√	Buypass CA utsteder og administrerer kvalifiserte sertifikater. Buypass CA produserer lister over sperrede sertifikater (CRL). CRLene er tilgjengelig fra Buypass' nettsider.	
LRA-klient	√	√	√	LRA-klienten inneholder funksjonalitet for å utstede og administrere lokale og kvalifiserte sertifikater. En LRA-klient må ha følgende periferutstyr for å fungere: Skanner, signaturplate, PIN-kode tastatur, samt 2 kortlesere. Kontrolldokumenter (pdf) lagres på et sikkert filområde.	LRA-klienten installeres på en eller flere PC-er med Windows Win7 eller Win8 32- eller 64-bits.
Smartkort	√	√	√	Buypass Smartkort som er bærer av både lokale og kvalifiserte sertifikater.	Smartkortet tilpasses bedriftens krav ifht andre bruksområder.
NetID Enterprise	√	√	√	Programvare som kommuniserer med smartkortet. Installeres på arbeidsstasjoner og / eller terminalservere slik at bruker kan benytte smartkort/sertifkater til blant annet pålogging og signering.	

6 Elementer i en implementeringsplan

For implementering av smartkort og sertifikater i bedriften bør følgende steg gjennomføres for å sikre en vellykket implementering.

Punktene nevnte er eksempler og må ikke ses som en fullstendig eller uttømmende liste. Buypass eller Buypass partner kan bidra i gjennomføringen.

6.1 Kartlegging – smartkort

Oppgaver og aktiviteter i ulike faser	Kommentarer
Kartlegge hvilke ønsker / krav bedriften har til smartkortets funksjoner	• Visuelt: Bilde, signatur, brukerinformasjon, bedriftslogo, strekkode, etc. • Adgangskontroll – berøringsfri eller bruk av magnetstripe • Magnetstripe og funksjonalitet for kantinebetaling, kopimaskiner, etc. • Chip og behov for ulike sertifikattyper
Kartlegge hvilke systemer/programvare bedriften benytter som har krav til bruk av lokale og/eller kvalifiserte sertifikater	Fagsystemer internt og eksternt.
Kartlegge lokal CA og identifisere behov for endringer/tilpasninger	Root-CA, issuing CA, soneplassering, vurdere CP/CPS, bestemme verdier for de ulike sertifikattypene LRAen benytter, etc.
Kartlegge lokal AD og identifisere behov for endringer/tilpasninger	Designe bruker- og gruppeprofiler i AD, bestemme informasjonsinnhold og eventuelt bruk av nye attributter, oppdatere brukerinformasjon og tilordne roller/grupper til brukerne
Kartlegge bedriftens IT-infrastruktur mhp bruk av smartkortet	Diskkryptering, domenepålogging, SSO, VPN og klienttyper
Kartlegge bedriftens IT-infrastruktur mhp behov ny eller endringer av soneinndeling, port- og brannmuråpninger	Sikre og usikrede soner. Hvor ligger brukere og ressurser
Identifisere behov for / vurdere bedriftsspesifikke tilpasninger av Buypass Access Enterprise (CSP)	Sees i sammenheng med punktene over

6.2 Kartlegging – ID-kontoret og klienttilpasninger

Oppgaver og aktiviteter i ulike faser	Kommentarer
Dersom bedriften har ID-kontor må det vurderes behov for endringer. Om eget ID-kontor ikke eksisterer må det vurderes hvordan smartkort-administrasjonen skal gjennomføres	Lokasjon, åpningstider, bemanning
Kartlegge behov for en eller flere LRA-klienter og/eller bruk av distribuert funksjonalitet	Sees i sammenheng med punktet over
Kartlegge og vurdere antall og behov for anskaffelse av LRA-PCer, kortlesere, PIN-tastatur, skannings- og signaturutstyr	Sees i sammenheng med punktet over

Oppgaver og aktiviteter i ulike faser	Kommentarer
Identifisere behov for / vurdere bedriftsspesifikke tilpasninger i forhold til konfigurering av LRA-klient	Konfigurasjonsguide tilgjengelig
Identifisere behov for / vurdere bedriftsspesifikke tilpasninger i forhold til interne rutiner og prosedyrer for utstedelse og administrasjon av smartkort og sertifikater	Rutiner: • Tiltreden/fratreden • Mistet/stjålet kort • Fornyelse av sertifikater og kort • Lånekort • Permisjoner • Endring av brukerinformasjon og sertifikattilganger m.m. i AD i tilknytning til kort og sertifikater • Legitimasjonskontroll lokale sertifikater • Legitimasjonskontroll kvalifiserte sertifikater • Brukervilkår for lokale sertifikater • Avtalevilkår for kvalifiserte sertifikater • Utnevnelse og administrering av RA-ADMIN og LRA Operatører

6.3 Test - pilotdrift

Teori og praksis er ikke det samme. I en kartleggingsfase er det vanskelig å huske på alle forhold som kan spille inn. Det er derfor viktig å gjennomføre tilstrekkelig med tester i et miljø som gjenspeiler det miljøet bedriften ønsker å rulle ut for bruk av lokale og kvalifiserte sertifikater.

Testfasen vil ofte kjøres som pilotdrift, hvor bedriften ikke setter opp eget testmiljø, men kjører på en tidlig fase av ønsket produksjonsmiljø.

Oppgaver og aktiviteter i ulike faser	Kommentarer
Bedriftens må sette opp et miljø med alle nye komponenter	Mulige komponenter: • Lokal CA med tilhørende CRL • Nødvendige endringer i AD • Installere LRA-klient med periferutstyr • Installere Buypass Access/NetID Enterprise på arbeidsstasjoner og eventuelle terminalservere – demoversjoner er tilgjengelig (90 dager) • Brannmuråpning – tilgang til Buypass
Teste alle påloggingsscenarioer	
Teste alle signerings- og krypteringsscenarioer	
Teste alle infrastrukturendringer, soneinndelinger, port- og brannmuråpninger	
Vurdere om løsningen tilfredsstiller bedriftens behov	
Utarbeide innføringsplan basert på testresultatene	I noen tilfeller må korrigerende tiltak iverksettes før smartkort og sertifikater tas i bruk

6.4 Produksjon – oppstart

Oppgaver og aktiviteter i ulike faser	Kommentarer
Bestille Buypass Access Enterprise (NetID)	Eget skjema tilgjengelig for utfylling. Inngå avtale med Buypass på antall lisenser
Bestille smartkort	Smartkort kan ha flere ukers leveringstid avhengig av funksjonalitet
Bestille LRA-klient og periferutstyr	Inngå avtale med Buypass om antall klienter
Implementere nødvendige system- og programvareendringer basert på overgang til bruk av sertifikater	
Implementere nødvendige infrastrukturendringer, soneinndelinger, port- og brannmuråpninger basert på overgang til bruk av sertifikater	
Utarbeide og implementere ny eller endret CP/CPS for lokal MS CA – kun om det ønskes av bedriften	Se http://www.buypass.no/kundeservice/nedlastingssenter og CA Dokumenter (juridisk)
Installere/utføre endringer lokal CA	
Installere/utføre endringer i AD	
RA-avtale må inngås med Buypass for delegering av ansvar for utstedelse av kvalifiserte sertifikater	Avtaleutkast er tilgjengelig
Nye roller beskrives og bemannes	RA-ADMIN og LRA Operatør
Utarbeide og implementere nye og/eller endrede rutiner for administrering av brukere, smartkort og sertifikater. I den første fasen spesielt med tanke på nyutstedelse av kort og sertifikater	
Bedriftens system-, drift- og brukerdokumentasjon utarbeides / oppdateres – kun om det ønskes av bedriften	Teknisk dokumentasjon og brukerdokumentasjon for LRA-klienten foreligger – se dokumentreferanser gitt i egen oversikt
Gjennomføre opplæring for nøkkelpersonell; for eksempel CA/AD-admin, RA-ADMIN og LRA Operatører	Gjennomføres av personell fra Buypass i samarbeid med ansvarlige for implementeringen fra bedrifter
Planlegge trinnvis innføring av smartkort i bedriften	Gjerne inklusive pilotering. Utarbeid stoppkriterier under utrulling

6.5 Produksjon – utrulling

Oppgaver og aktiviteter i ulike faser	Kommentarer
Installere LRA-klient med ønskede konfigureringstilpasninger	
Installere NetID Enterprise på arbeidsstasjoner og terminalservere	
Innføre løsningen for pilotgruppe	
Korrigere infrastruktur og rutiner dersom nødvendig basert på tilbakemelding fra pilotgruppe	
Innføre løsningen trinnvis i bedriften	

6.6 Produksjon – oppfølging

Oppgaver og aktiviteter i ulike faser	Kommentarer
Iverksette driftsrutiner inkludert backup og failoverprosedyrer for • CA m/CRL • AD • LRA-klient m/dokumentregister	
Iverksette rutiner for administrering av brukere, smartkort og sertifikater. I denne fasen spesielt med tanke på daglig drift og vedlikehold ifbm sperring av sertifikater og erstatningskort, fornyelser og endringer av brukerinformasjon	