
Cybernetica AS

E-hääletamise süsteem

Valijarakenduse pakendamine

Version 2.5

Dokument: EHA-03-04-2.5

Kuupäev: 22.04.2014

E-hääletamise süsteem	Versioon: 2.5
Valijarakenduse pakendamine	Kuupäev: 22.04.2014

Redaktsioonide ajalugu

Kuupäev	Versioon	Kirjeldus ja muudatused	Autor
4.12.2010	2.0	Dokumendi algatamine.	Sven Heiberg
5.12.2010	2.1	Koostatud dokument.	Sven Heiberg
13.12.10	2.2	Redigeeritud dokument.	Samuel Paal
11.08.2013	2.3	KOV 2013	Sven Heiberg
18.09.2013	2.4	Täpsustused	Sven Heiberg
22.04.2014	2.5	Kirjeldatud muutunud kasutajaliides Kirjeldatud UPX integreerimine Kirjeldatud MacOS allkirjastamine ja pakendamine	Sven Heiberg

Sisukord

1 Ülevaade.....	4
1.1 Pakendamise põhimõte.....	4
1.2 Pakendatavad komponendid.....	4
1.3 Vajalikud tööriistad.....	5
2 Ressursside seadistamine.....	5
2.1 Seadistaja.exe.....	5
2.2 Ressursside tüübid.....	7
2.3 Tekstide maskid.....	8
2.4 Vaadete redigeerimine.....	9
3 Seadistuste rakendamine.....	9
4 Valija rakenduse allkirjastamine.....	10
4.1 Sissejuhatus.....	10
4.2 Windows.....	10
4.2.1 Eeldused.....	10
4.2.2 Allkirjastamine.....	11
4.3 MacOS X.....	12
5 Pakendatud rakenduse testimine.....	12
6 Lisa 2 – Toetatud HTML alamhulk.....	14

1 Ülevaade

1.1 Pakendamise põhimõte

Valijarakendus kasutab enda töös seadistatavaid ressursse, mille abil kujundatakse Valijarakenduse lõplik väljanägemine ning täpsustatakse konkreetse(te)l hääletus(t)el osalemiseks vajalikud parameetrid. Valijarakenduse käimasoleva(te)ks hääletus(t)eks töökorda seadmist nimetame Valijarakenduse pakendamiseks.

Valijarakenduse pakendamine koosneb järgmistest tegevustest

- Seadistuste koostamine
- Seadistuste rakendamine
- Rakenduse signeerimine
- Pakendatud rakenduse testimine

Valijarakendus on kõigi platvormide tarbeks seadistatav Windows platvormil.

1.2 Pakendatavad komponendid

Valijarakenduse pakendamise käigus seadistatakse alljärgnevat komponente:

- Windows rakendus – valimine.exe
- Linux 32bit rakendus – valimine32.bin
- Linux 64bit rakendus – valimine64.bin
- Mac OS X rakendus – Valimine
- Veebilehed

Seadistamine eeldab kompileeritud kuid seadistamata Valijarakenduse olemasolu. Seadistamiskõlblikud Valijarakendused eri platvormidele tarnitakse E-hääletuse CD'l.

Kui teistel platvormidel on Valijarakendus üks käivitav fail, siis MacOS X puhul koosneb rakendus mitmest failist. Rakenduse seadistamist vajav komponent paikneb failis:

Valimine

Rakenduse pakendamisel on vaja ka täiendavat faili, mis sisaldab OS X spetsiifilisi ressursse:

Valimine.tar

1.3 Vajalikud tööriistad

Valijarakenduse pakendamiseks vajalikud tööriistad tarnitakse E-hääletuse CD-l.

- **Seadistaja.exe** – Seadistaja on programm, mille abil on võimalik luua ja redigeerida Valijarakenduse ressurssifaile, ressursse Valijarakendusse süstida ja vajadusel pakitud Valijarakenduse kontrollsummat uuendada
- **upx.exe** – Valija rakenduse binaaride pakkimiseks võib kasutada utiliiti UPX (the Ultimate Packer for Executables, <http://upx.sourceforge.net/>). Tegemist on exe-pakkijaga, mille töö jääb lõppkasutajale nähtamatuks - pakitud programm pakib ennast ise enne käivitumist lahti, ilma et kasutaja midagi tegema peaks.
- **signtool.exe** – Utiliit Valijarakenduse Windows versioonide signeerimiseks
- **packagesigner.sh** – Utiliit Valijarakenduse MacOS X versiooni signeerimiseks ja pakendamiseks

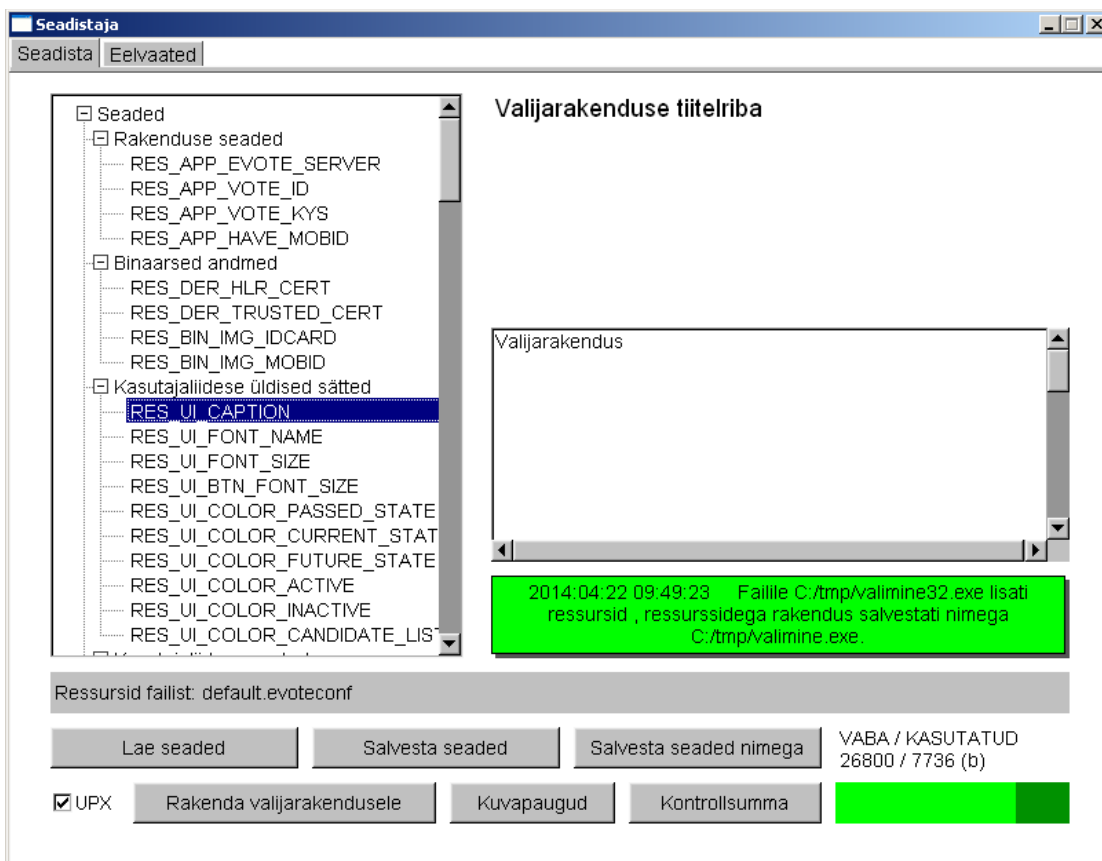
NB! Pakendamise õnnestumiseks peavad Seadistaja.exe ja upx.exe asuma samas kataloogis.

2 Ressursside seadistamine

2.1 Seadistaja.exe

Kõiki Valijarakenduse muudetavaid ressursse saab töödelda rakenduse Seadistaja.exe abil. Utiliit pakub järgnevat funktsionaalsust:

- Valijarakenduse ressurssifaili loomine vaikeseadistuste põhjal
- Valijarakenduse ressurssifaili redigeerimine ja salvestamine
- Muudatuste mõju jälgimine WYSIWYG meetodil
- Ressursside rakendamine Valijarakendusele
- UPX pakkimise rakendamine Valijarakendusele
- Valijarakenduse kontrollsumma uuendamine

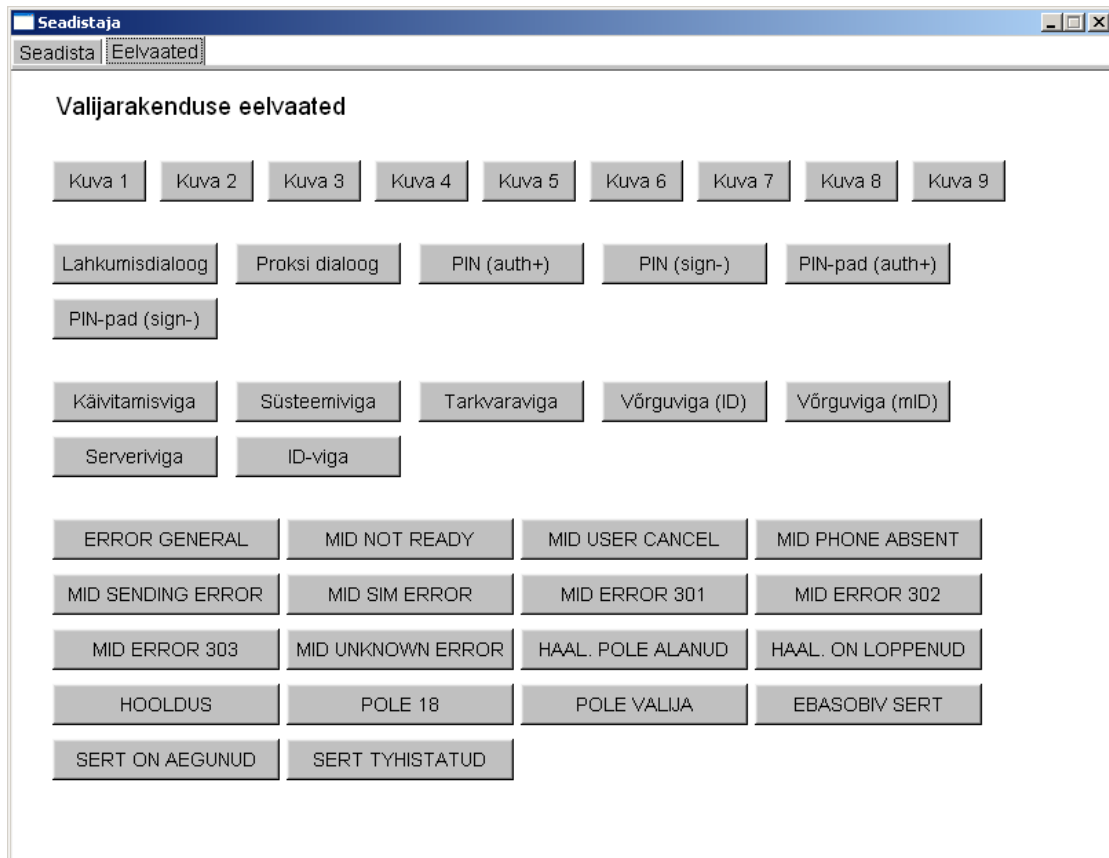


Ressursside redigeerimine

Seadistaja vaates „Seadista“ on võimalik redigeerida ressursse. Vaates kuvatakse:

1. Seadistatavate ressursside nimekiri.
2. Valitud ressursi redigeerimise ja info paneel.
 - 2.1. Ressursi kirjeldus
 - 2.2. Ressursi kuva/redigeerimisala. Vastavalt ressursi sisutüübile (vt. 2.2):
 - a) RES_TEXT – tekstikast, mis võimaldab tekstisisestust
 - b) RES_NUMBER – tekstikast, mis võimaldab numbrite sisestust
 - c) RES_BOOLEAN – „radio“ nupud JAH/EI vastuse valimiseks
 - d) RES_IMAGE_BMP – kuvatakse pilt
 - e) RES_CERT – mitteredigeeritav tekstikast serdi kirjeldusega
 - 2.3. Ressursi redigeerimise nupud vastavalt ressursi sisutüübile:
 - a) RES_IMAGE_BMP, RES_CERT:
„Lae failist“ - avab dialoogi, mis võimaldab valida faili
„Kustuta“ - kustutab ressursi väärtuse
 - b) RES_COLOR:
„Vali“ - avab värvipaletiga dialoogi, mis võimaldab värvi valida
3. Administreerimis- ja infopaneel. Sisaldab administreerimiseks kasutatavaid nuppe ning infot seadistuste hetkeoleku kohta.
 - 3.1. Infotabloo, mis kajastab infot seadistustoimingute kohta. Paneeli värv tähistab:
Roheline – toiming õnnestus
Punane – toiming ebaõnnestus

- 3.2. Seadistusfaili nimi, mida redigeeritakse. Paneeli värv tähistab:
Valge – ressursid on seadistusfaili salvestatud
Punane – ressursid on seadistusfaili salvestamata
Hall – töötatakse vaikeressurssidega, seadistusfail on salvestamata
- 3.3. Ressursside kasutamata/kasutatud ruum baitides. Diagrammi värvid tähistavad:
Heleroheline – vaba ruum
Tumeroheline – kasutatud ruum



Eelvaated

Seadistaja vaates „Eelvaated“ on võimalik vaadata redigeeritud ressursside toimet valijarakenduses. Vaates kuvatakse nupud

1. kõigi kuvade aktiveerimiseks,
2. kõigi dialoogiakende aktiveerimiseks,
3. kõigile vealiikidele vastavate vaadete aktiveerimiseks ja
4. kõigi serveri poolt indikeeritud veasituatsioonidele vastavate veavaadete aktiveerimiseks.

Tähelepanu: Dokumendis olevatel ekraanitõmmistel on illustreeriv otstarve. Ekraanitõmmiste ja selgitava teksti lahknevuste korral tuleb lähtuda tekstist.

2.2 Ressursside tüübid

Valijarakenduse seadistatavad ressursid jagunevad järgmistesse tüüpidesse:

- **RES_TEXT**: Kõik valijarakenduses kasutatavad stringid – veateated, kasutajaliidese tekstid, tekstide maskid. Vahetu redigeerimine võimalik.
- **RES_NUMBER**: Fontide suurused ja teised numbrilised andmed. Vahetu redigeerimine võimalik.
- **RES_BOOLEAN**: Tõeväärtustüüpi kasutatakse Mobiil-ID seadistustes sisse-/väljalülitamiseks. Vahetu redigeerimine võimalik.
- **RES_IMAGE_BMP**: ID-kaardi ja Mobiil-ID ametlikud pildid lisatakse rakendusele BMP vormingus piltidena. Vahetu redigeerimine ei ole võimalik, pilte saab lisada ja eemaldada. NB! Valijarakendus eeldab piltidelt suurust 160 x 64 pikselit.
- **RES_CERT**: HLR ja HES sertifikaat salvestatakse ressursidesse DER kodeeritud kujul. Vahetu redigeerimine ei ole võimalik, serti saab lisada ja eemaldada. Sisendandmed võivad olla nii DER kui PEM vormingus.
- **RES_COLOR** : Fontide värvid, tekstide värvid. Vahetu redigeerimine võimalik.

2.3 Tekstide maskid

Valijarakenduses on töö käigus genereeritavad dünaamilised tekstid ja nende kujundus teineteisest lahus. Tekstiväli sisaldab puhast teksti, teksti *mask* sisaldab HTML-märgendeid, millega tekst on kujundatud ja kohahoidjaid dünaamilise teksti süstimiseks.

Kohahoidjad kirjeldatakse kujul %i%, kus i on täisarv. Nt. %1%

Näiteks kui on defineeritud tekst:

```
"Teie valik on:"
```

ja teksti mask:

```
"%1%<b>Kandidaat number %2%</b>"
```

Siis pannakse need, eeldusel et valisite kandidaadi number XXX, rakenduses kokku:

```
Teie valik on:<b>Kandidaat number XXX</b>
```

Selle tulemusena kuvatakse tekst rasvases kirjas ().

NB! Maske redigeerides peab kohahoidjate arv säilima muutumatuna, vastasel juhul rakendus keeldub töötamast. Kohahoidjate loendamine algab 1'st.

Staatiliste tekstide korral kasutatakse HTML-märgendeid otse tekstis.

Toetatud alamhulk HTML keele elementidest on kirjeldatud lisas 2.

2.4 Vaadete redigeerimine

Seadistamise töövoog näeb lihtsustatult välja nii:

- Käivita Seadistaja.exe.
- Kui on olemas seadistusfail, siis lae see Seadistajasse (<Lae seaded>).
- Kui seadistusfaili ei ole, siis kuvatakse vaikeseaded, mille salvestamisel (<Salvesta seaded>) tekib uus seadistusfail (vaikimisi default.evotefconf).
- Redigeeri seadeid – iga ressurssiga kaasneb info – kus antud seadistust kasutatakse ja kuidas.
- Salvesta (<Salvesta seaded>, <Salvesta seaded nimega>)
- Klõpsat huvipakkuva vaate nupul ning veendu, kas tulemus on ootuspärane ja meeldiv.

3 Seadistuste rakendamine

Sobiva seadistusfaili olemasolu korral on võimalik Valijarakenduse tegelik seadistamine. Selle protseduuri käigus süstitakse seadefailis salvestatud seaded Valijarakenduse binaari ning arvutatakse muudetud binaarile kontrollsumma. Seadistuste rakendamine on platvormist sõltumatu nt. võib MacOS X universaalbinaari seadistada Windows platvormil.

Vajadusel Valijarakendus UPX-pakitakse. MacOS X platvormil saab UPX pakkimisest loobuda juhul kui rakenduse levitamiseks kasutatakse DMG kettatõmmist.

- Käivita Seadistaja.exe
- Lae seadistusfail. (<Lae seaded>)
- Veendu visuaalsel vaatlusel, et laadised õige seadistusfaili ja et seaded on korrektsed.
- Kui soovid koos seadistamisega rakendada ka UPX pakkimist, siis tee linnuke kasti <UPX>
- Klõpsa nupul <Rakenda valijarakendusele>
- Vali puhas fail, mida soovid ressurssidega täiendada, klõpsa <OK>
- Vali tekitatava faili nimi, klõpsa <OK>
- Seaded süstitakse Valijarakendusse, ühtlasi uuendatakse kontrollsumma. Vajadusel rakendatakse pakkimist.

Seadistuste rakendamise järel on Valijarakendus kasutamiseks valmis. Valikuliselt võib Valijarakendust enne evitamist ka digitaalselt allkirjastada.

4 Valija rakenduse allkirjastamine

4.1 Sissejuhatus

Valijarakenduse tervikluse tagamine on e-hääletuse kontekstis äärmiselt oluline. Valijarakendus kontrollib ise töö käigus oma kontrollsummat ja saadab kontrolli tulemuse hääleedastusserverile. Samas on Windows ja Mac OS platvormidel väljakujunemas levinud meetodid koodi digitaalseks allkirjastamiseks ja/või ajatembeldamiseks.

4.2 Windows

4.2.1 Eeldused

Windows platvormil on võimalik Valijarakenduse digitaalne allkirjastamine. Seadistaja.exe kontrollsumma arvutamine oskab arvestada võimalusega, et Valijarakendusele lisatakse hiljem digiallkiri ja seega ei kaota kontrollsumma peale binaari muutmist allkirja võrra oma kehtivust.

Allkirjastamiseks on vaja järgmisi vahendeid.

1. Allkirjastamisvõti
2. Tarkvara allkirjastamisvõtme kasutamiseks Windows platvormil
3. Internetiühendus (vajalik ajatembelduseks)
4. Utiliiti signtool.exe, mis tarnitakse E-hääletuse CD-l
5. Seadistatud ja UPX-pakitud `valimine.exe` fail.

4.2.2 Allkirjastamine

Valija rakenduse allkirjastamiseks tehke järgnevat.

1. Aktiveerige allkirjastamisvõti
2. Käivitage rakendus `signtool.exe`:

> signtool sign /n <allkirjastaja> /t <ajatempliteenuse URL> /d <kirjeldus> /du <Valimiste URL> <allkirjastatav fail>

<allkirjastaja> - Osa allkirjastava sertifikaadi subjekti nimest, sertifikaat peab võimaldama koodi signeerimist ning olema registreeritud allkirjastamiseks kasutatavas masinas

<ajatempliteenuse URL> - Näiteks:

`http://timestamp.verisign.com/scripts/timestamp.dll`

<kirjeldus> - Näiteks: „Valijarakendus“

<Valimiste URL> - Veebilehe URL, kus on rakenduse räsid, avalikud võtmed jm.

Näiteks: `http://www.valimised.ee/`

3. Käituge vastavalt juhistele ekraanil. Allkirjastamise õnnestumisel kuvatakse teade: "Successfully signed and timestamped". Sellega on rakendus allkirjastatud.
4. Korrake eelnenud samme teiste signeeritavate failidega.

4.3 MacOS X

MacOS X platvormil on rakenduse allkirjastamine ja pakendamine seotud üheks tegevuseks.

MacOS X Gatekeeper piirab üldjuhul paigaldatava tarkvara MacStore'ist pärinevate või Apple'i poolt registreeritud arendajate rakendustega. Allkirjastada saab ka teiste koodisigneerimisvõtmetega, kuid need ei ole MacOS X platvormil tunnustatud. Seetõttu võib osutuda otstarbekaks lasta MacOS X rakendus allkirjastada arendajal.

Olenemata allkirjastajast on allkirjastamiseks vaja järgmisi vahendeid.

1. Allkirjastamisvõti
2. Tarkvara allkirjastamisvõtme kasutamiseks MacOS platvormil
3. Utiliiti `packagesigner.sh`, mis tarnitakse E-hääletuse CD-l
4. MacOS ressursid, mis tarnitakse E-hääletuse CD-l pakis `Valimine.tar`
5. Seadistatud fail `Valimine`

Valija rakenduse allkirjastamiseks tehke järgnevat.

5. Aktiveerige allkirjastamisvõti
6. Käivitage utiliid `packagesigner.sh`, samas kaustas failidega `Valimine` ja `Valimine.tar`

> packagesigner.sh Valimine <allkirjastaja>

<allkirjastaja> - Osa allkirjastava sertifikaadi subjekti nimest, sertifikaat peab võimaldama koodi signeerimist ning olema registreeritud allkirjastamiseks kasutatavas masinas.

Tulemusena tekib valijarakenduse paigalduspakk `valimine.dmg`

5 Pakendatud rakenduse testimine

Pärast Valijarakenduse kohandamist tuleb seda alati testida, et veenduda muudatuste korrektsuses. Selleks tuleb läbi viia testhääletamine ja häälte lugemine; veenduda, et häälte dekrüpteerimine õnnestub ning et hääletustulemused vastavad hääletamisel tehtud valikutele.

Täiendavalt on oluline jälgida, et Valijarakenduse kontrollsummad oleksid korrektsed ning allkirjad verifitseeruks. Hääleedastusserveris tuleb veenduda, et kliendikontrollilogi oleks ootuspärane.

6 Lisa 2 – Toetatud HTML alamhulk

Märgendid:

- A: HREF/NAME
- B
- BODY: BGCOLOR/TEXT/LINK
- BR
- CENTER
- CODE
- DD
- DL
- DT
- EM
- FONT: COLOR/SIZE/FACE=(helvetica/arial/sans/times/serif/symbol/courier)
- H1/H2/H3/H4/H5/H6
- HEAD
- HR
- I
- IMG: SRC/WIDTH/HEIGHT/ALT
- KBD
- LI
- OL
- P
- PRE
- STRONG
- TABLE: TH/TD/TR/BORDER/BGCOLOR/COLSPAN/ALIGN=CENTER|RIGHT|LEFT
- TITLE
- TT
- U
- UL
- VAR

Värvide nimetused:

- black,red,green,yellow,blue,magenta,fuchsia,cyan,aqua,white,gray,grey,lime,maroon,navy,olive,purple,silver,teal.

URL tüübid:

- Internal: file:
- External: http: ftp: https: ipp: mailto: news:

Sümbolviited:

- Aacute aacute Acirc acirc acute AElig aelig Agrave agrave amp Aring aring
Atilde atilde Auml auml
- brvbar bull
- Ccedil ccedil cedil cent copy curren
- deg divide
- Eacute eacute Ecirc ecirc Egrave egrave ETH eth Euml euml euro
- frac12 frac14 frac34
- gt
- Iacute iacute Icirc icirc iexcl Igrave igrave iquest Iuml iuml
- laquo lt
- macr micro middot
- nbsp not Ntilde ntilde
- Oacute oacute Ocirc ocirc Ograve ograve ordf ordm Oslash oslash Otilde
otilde Ouml ouml
- para premil plusmn pound
- quot
- raquo reg
- sect shy sup1 sup2 sup3 szlig
- THORN thorn times trade
- Uacute uacute Ucirc ucirc Ugrave ugrave uml Uuml uuml
- Yacute yacute
- yen Yuml yuml