Systémové programování Windows

Event Log

Obsah

- Prohlížení event logů
- Vytvoření event logu
- Message file
  - Tvorba
  - Registrace

Prohlížení event logu

- Eventvwr.msc
- Windows logs
  - Application
  - System
  - Security

Vytvoření event logu

```
HANDLE RegisterEventSource(
        PCTSTR machineName,
        PCTSTR sourceName );

BOOL ReportEvent(
        HANDLE hEventLog,
        WORD eventType, // EVENTLOG_INFORMATION_TYPE
        WORD eventCategory, // CATEGORY_1 z .mc
        DWORD eventID, // EVENT_2_ERROR z .mc
        PSID userSid,
        WORD numStrings,
        DWORD dataSize,
        PCTSTR* strings,
        PVOID rawData );
```

Message Text File (.mc)

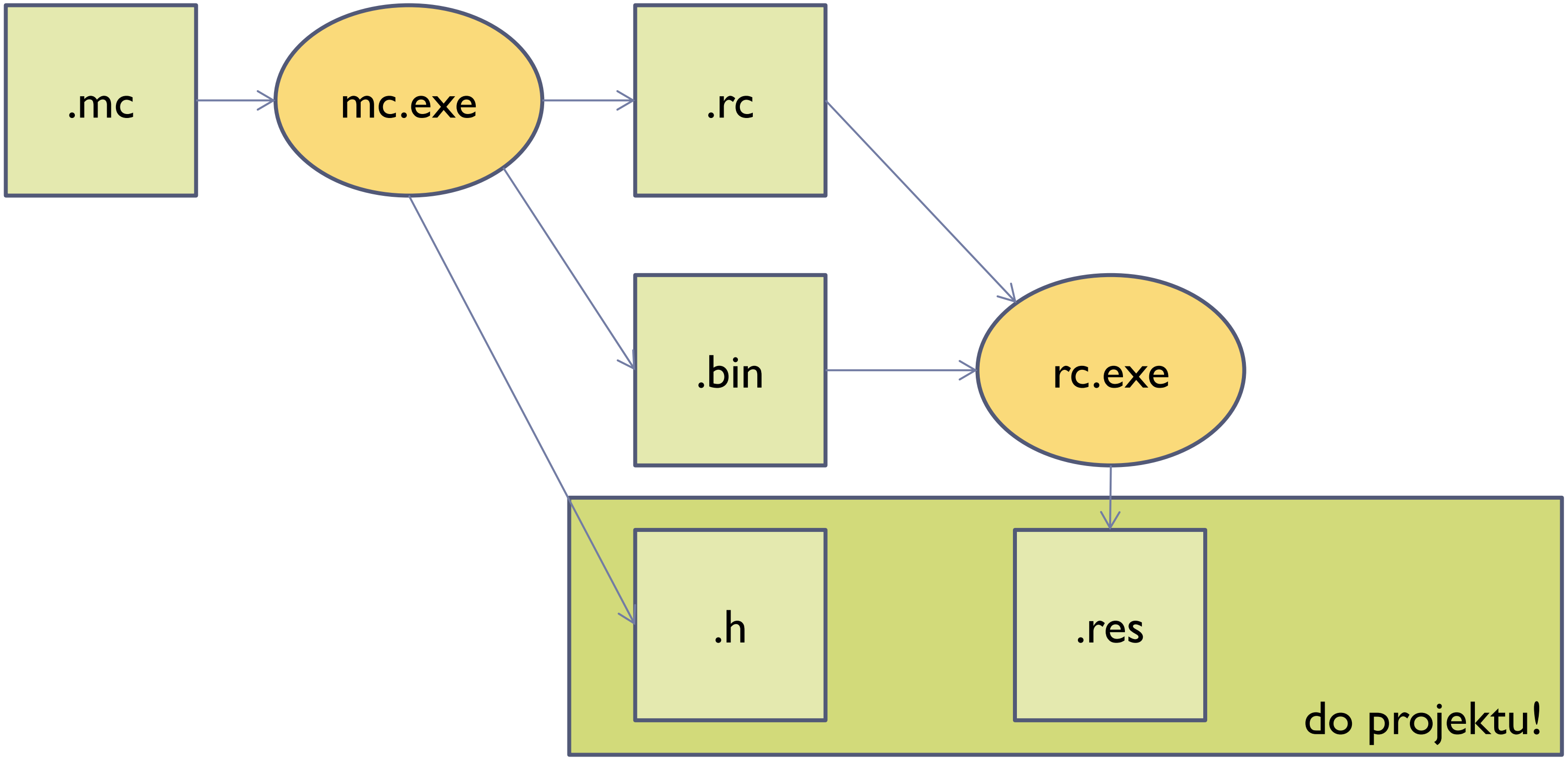
- Definuje texty
  - Kategorie
  - Události
  - Parametry
- Vícejazyčný
- Pozor na syntaxi

Message Text File (.mc)

- Událost

```
MessageId=0x10
Severity=Informational
Facility=Application
SymbolicName=EVENT_1_INFO
Language=English
Event 1 - info
.
```

Tvorba Message File



C:\Program Files\Microsoft SDKs\Windows\v7.0A\bin\
C:\Program Files\Windows Kits\8.0\bin\x86\

Registrace

- HKEY_LOCAL_MACHINE
  - SYSTEM
    - CurrentControlSet
      - Services
        - EventLog
          - Application
            - *Event Source*

Registrace

- EventMessageFile [REG_EXPAND_SZ]
  - Stores the location of the file containing categories for the events generated by the source program.
- CategoryMessageFile [REG_EXPAND_SZ]
- ParameterMessageFile [REG_EXPAND_SZ]

- TypesSupported [REG_DWORD] 7
  - Indicates the types of events generated by the source program.
- CategoryCount [REG_DWORD]
  - Specifies the number of event categories defined by the source program.

Díky za pozornost