

Konfigurácia autentifikácie

- [Príklady konfigurácie](#)
 - [Jednoduchá autentifikácia cez D2000 používateľov](#)
 - [Jednoduchá autentifikácia cez aplikácie definovaných používateľov](#)
 - [Autentifikácia cez D2000 používateľov a lokálne overovanie klientských certifikátov](#)
 - [Autentifikácia cez D2000 používateľov a vzdialené overovanie klientských certifikátov](#)
 - [Autentifikácia cez aplikácie definovaných používateľov a lokálne overovanie klientských certifikátov](#)
 - [Autentifikácia cez aplikácie definovaných používateľov a vzdialené overovanie klientských certifikátov](#)
 - [Single Sign On autentifikácia cez SPNEGO token](#)
 - [Automatická autentifikácia cez preddefinovaného D2000 používateľa bez prihlasovacej obrazovky](#)

Konfigurácia autentifikácie SmartWeb aplikácie má nasledovnú štruktúru v súbore `smartweb.json`. Príklady konfigurácie sú uvedené nižšie.

smartweb.json

```

{
    /* objekt s konfiguráciou autentifikácie používateľov */
    "authentication": {
        "authModes": [
            "AUTH_AUTO_LOGON_IN_SESSION",          // automatické prihlásenie do D2000 bez zobrazenia
            prihlasovacej obrazovky
            "AUTH_CREDENTIALS_IN_SESSION", // autentifikácia mena/hesla k D2000 používateľovi
            "AUTH_CREDENTIALS_IN_RPC",          // autentifikácia mena/hesla cez RPC
            (aplikane definovaný používateľia)
            "AUTH_CERTIFICATE_LOCALLY",         // autentifikácia certifikátu k lokálnemu keystore
            "AUTH_CERTIFICATE_REMOTELY",        // autentifikácia certifikátu cez RPC ku keystore
            spravovanému v D2000
            "AUTH_SPNEGO_REMOTELY",             // Single Sign On autentifikácia cez SPNEGO token
            posielany do D2000 na overenie
        ],

        // definícia D2000 používateľa na vytvorenie JAPI session
        // iba pre mód AUTH_AUTO_LOGON_IN_SESSION alebo AUTH_CREDENTIALS_IN_RPC
        "authSessionUsername": "D2000UserName", // používateľské meno do D2000
        "authSessionPassword": "D2000UserPassword", // heslo do D2000

        // cesta ku keystore a koreový certifikát na validáciu klientských certifikátov
        // iba pre mód AUTH_CERTIFICATE_LOCALLY
        "keystorePath": "C:\cesta ku keystore\keystore.jks",
        "caCertificateAlias": "SmartWebUsersCert", // alias koreového certifikátu v keystore.
        jks,

        // definícia autentifikanej RPC, iba pri zapnutom móde AUTH_CREDENTIALS_IN_RPC
        "authRpc": {
            "eventName": "E.SMARTWEB_USER",
            "interfaceName": "I.XXX",
            "methodName": "authenticate",
            "useJava": "false"
        },
        "authRpcParams": [ // poradie parametrov volanej autentifikanej metódy, povinný je len OUT
            parameter _OK (BOOL);
            "USERNAME",
            "PASSWORD",
            "CERTIFICATE",
            "NONE",
            "_OK"
        ],

        // definícia logOn RPC metódy, volaná automaticky po úspešnej autentifikácii, nepovinný OUT
        parameter _OK (BOOL) identifikuje úspešnosť volania logOn metódy;
        "logOnRpc": {
            "eventName": "E.SW_DT_Connect",
            "interfaceName": "I.XXX",
            "methodName": "logOn",
            "useJava": "false"
        },
        "logOnRpcParams": [ // poradie parametrov volanej logOn metódy, povinný je len OUT parameter _OK
            (BOOL);
            "USERNAME",
            "PASSWORD",
            "CERTIFICATE",
            "NONE",
            "_OK"
        ],

        "logOutRpc": {
            "eventName": "E.SW_DT_Connect",
            "interfaceName": "I.XXX",
            "methodName": "logOff",
            "useJava": "false"
        }
    }
}

```

Príklady konfigurácie

Jednoduchá autentifikácia cez D2000 používateľov

smartweb.json

```
{
  "authentication": {
    "authModes": [
      "AUTH_CREDENTIALS_IN_SESSION"
    ]
  }
}
```

Jednoduchá autentifikácia cez aplikane definovaných používateľov

V nasledujúcej konfigurácii je navyše zaregistrovaná aj "logOn" metóda z dôvodu identifikácie [aktuálne prihláseného používateľa vo volaných RPC metódach](#).

smartweb.json

```
{
  "authentication": {
    "authModes": [
      "AUTH_CREDENTIALS_IN_RPC"
    ],
    // preddefinované username D2000 používateľa s ktorým sa bude vytvára session
    "authSessionUsername": "D2000UserName",
    // preddefinované heslo D2000 používateľa s ktorým sa bude vytvára session
    "authSessionPassword": "D2000UserPassword",

    // definícia autentifikanej RPC
    "authRpc": {
      "eventName": "E.SW_APPLICATION_AUTH",
      "methodName": "authenticate"
    },
    "authRpcParams": [
      "USERNAME",
      "PASSWORD",
      "_OK"
    ],

    // definícia logOn RPC metódy
    "logOnRpc": {
      "eventName": "E.SW_APPLICATION_AUTH",
      "methodName": "logOn"
    },
    "logOnRpcParams": [
      "USERNAME",
      "_OK"
    ]
  }
}
```

Autentifikácia cez D2000 používateľov a lokálne overovanie klientských certifikátov

Overovanie klientských certifikátov prebieha lokálne v SmartWeb aplikácii. Všetky klientské certifikáty musia byť uložené v keystore pod aliasom identickým s prihlasovacím menom (pozor na case sensitivity) a musia byť podpísané koreovým certifikátom s menom definovaným v `caCertificateAlias` atribúte konfigurácie. Pre úspešnú konfiguráciu potrebne správne nakonfigurovať [element authentication v súbore standalone.xml](#) aplikovaného servera [Wildfly](#). Klientské certifikáty je potrebné generovať podľa postupu popísaného v kapitole [Správa klientských certifikátov](#).

smartweb.json

```
{
    "authentication": {
        "authModes": [
            "AUTH_CREDENTIALS_IN_SESSION",
            "AUTH_CERTIFICATE_LOCALLY"
        ],

        // cesta ku keystore s klientskými certifikátmi a koreovým certifikátom na validáciu
        klientských certifikátov
        "keystorePath": "C:\\cesta ku keystore\\keystore.jks",
        "caCertificateAlias": "SmartWebUsersCert" // alias koreového certifikátu v keystore.
    },
    jks,
}
```

Autentifikácia cez D2000 používateľov a vzdialené overovanie klientských certifikátov

Overovanie klientských certifikátov prebieha v D2000 volaním autentifikanej RPC metódy s parametrom, cez ktorý sa pošle Base64 serializovaný certifikát. Pre úspešnú konfiguráciu potrebné správne nakonfigurovať [element authentication v súbore standalone.xml aplikovaného servera Wildfly](#), kde keystore súbor musí obsahovať koreový certifikát s ktorým sú podpísané všetky klientské certifikáty.

smartweb.json

```
{
    /* objekt s konfiguráciou autentifikácie používateľov */
    "authentication": {
        "authModes": [
            "AUTH_CREDENTIALS_IN_SESSION",
            "AUTH_CERTIFICATE_REMOTELY"
        ],

        // definícia autentifikanej RPC
        "authRpc": {
            "eventName": "E.SW_APPLICATION_AUTH",
            "methodName": "authenticate"
        },
        "authRpcParams": [
            "USERNAME",
            "CERTIFICATE",
            "_OK"
        ]
    },
}
```

Autentifikácia cez aplikované definované používateľov a lokálne overovanie klientských certifikátov

Overovanie klientských certifikátov prebieha lokálne v SmartWeb aplikácii. Všetky klientské certifikáty musia byť uložené v keystore pod aliasom identickým s prihlasovacím menom (pozor na case sensitivity) a musia byť podpísané koreovým certifikátom s menom definovaným v caCertificateAlias atribúte konfigurácie. Pre úspešnú konfiguráciu potrebné správne nakonfigurovať [element authentication v súbore standalone.xml aplikovaného servera Wildfly](#). Klientské certifikáty je potrebné generovať podľa postupu popísaného v kapitole [Správa klientských certifikátov](#). V nasledujúcej konfigurácii je navyše zaregistrovaná aj "logOn" metóda z dôvodu identifikácie [aktuálne prihláseného používateľa vo volaných RPC metódach](#).

smartweb.json

```
{
  "authentication": {
    "authModes": [
      "AUTH_CREDENTIALS_IN_RPC",
      "AUTH_CERTIFICATE_LOCALLY"
    ],

    // preddefinované username D2000 používateľa s ktorým sa bude vytvára session
    "authSessionUsername": "D2000UserName",
    // preddefinované heslo D2000 používateľa s ktorým sa bude vytvára session
    "authSessionPassword": "D2000UserPassword",

    // cesta ku keystore s klientskými certifikátmi a koreovým certifikátom na validáciu
    klientských certifikátov
    "keystorePath": "C:\\cesta ku keystore\\keystore.jks",
    "caCertificateAlias": "SmartWebUsersCert", // alias koreového certifikátu v keystore.
    jks,

    // definícia autentifikanej RPC
    "authRpc": {
      "eventName": "E.SW_APPLICATION_AUTH",
      "methodName": "authenticate"
    },
    "authRpcParams": [
      "USERNAME",
      "PASSWORD",
      "_OK"
    ],

    // definícia logOn RPC metódy
    "logOnRpc": {
      "eventName": "E.SW_APPLICATION_AUTH",
      "methodName": "logOn"
    },
    "logOnRpcParams": [
      "USERNAME",
      "_OK"
    ]
  ]
}
```

Autentifikácia cez aplikane definovaných používateľov a vzdialené overovanie klientských certifikátov

Overovanie klientských certifikátov prebieha v D2000 volaním autentifikanej RPC metódy s parametrom, cez ktorý sa pošle Base64 serializovaný certifikát. Pre úspešnú konfiguráciu potrebné správne nakonfigurovať [element authentication v súbore standalone.xml](#) aplikovaného servera [Wildfly](#), kde keystore súbor musí obsahovať koreový certifikát s ktorým sú podpísané všetky klientské certifikáty. V nasledujúcej konfigurácii je navyše zaregistrovaná aj "logOn" metóda z dôvodu identifikácie [aktuálne prihláseného používateľa vo volaných RPC metódach](#).

smartweb.json

```
{
  /* objekt s konfiguráciou autentifikácie používateľov */
  "authentication": {
    "authModes": [
      "AUTH_CREDENTIALS_IN_RPC",
      "AUTH_CERTIFICATE_REMOTELY"
    ],

    // preddefinované username D2000 používateľa s ktorým sa bude vytvára session
    "authSessionUsername": "D2000UserName",
    // preddefinované heslo D2000 používateľa s ktorým sa bude vytvára session
    "authSessionPassword": "D2000UserPassword",

    // definícia autentifikanej RPC
    "authRpc": {
      "eventName": "E.SW_APPLICATION_AUTH",
      "methodName": "authenticate"
    },
    "authRpcParams": [
      "USERNAME",
      "PASSWORD",
      "CERTIFICATE",
      "_OK"
    ],

    // definícia logOn RPC metódy
    "logOnRpc": {
      "eventName": "E.SW_APPLICATION_AUTH",
      "methodName": "logOn"
    },
    "logOnRpcParams": [
      "USERNAME",
      "_OK"
    ]
  }
}
```

Single Sign On autentifikácia cez SPNEGO token

Pre funkciu Single Sign On autentifikácie je potrebné nastaviť [parameter na maske používateľa SPNEGO](#) a [parameter aplikácie AuthSecPrinc](#). Konfigurácia smartweb.json musí mať nasledovné parametre:

smartweb.json

```
{
  "authentication": {
    "authModes": [
      "AUTH_SPNEGO_REMOTELY",
      "AUTH_CREDENTIALS_IN_SESSION" // druhý mód autentifikácie je nevyhnutný iba pokiaľ
      // chceme povoliť aj prihlasovanie cez meno a heslo v prípade ak SSO autentifikácia zlyhala
    ],
  }
}
```

Automatická autentifikácia cez preddefinovaného D2000 používateľa bez prihlasovacej obrazovky

smartweb.json

```
{
  "authentication": {
    "authModes": [
      "AUTH_AUTO_LOGON_IN_SESSION"
    ],
    // preddefinované username D2000 používateľa s ktorým sa bude vytvára session
    "authSessionUsername": "D2000UserName",
    // preddefinované heslo D2000 používateľa s ktorým sa bude vytvára session
    "authSessionPassword": "D2000UserPassword"
  }
}
```