1. Įvadas. Trumpa Lotus Notes saugumo raida

1.1.1989: Notes versija 1.0

Nuo pat pradžių Lotus kompanija siekė savo produkte palaikyti aukštą duomenų saugumo lygį. išlaikyti duomenis saugius Saugumo savybės buvo galimos nuo pat pirmosios versijos dėka viešo rakto technologijos panaudojimo (RSA). Taip pat notes naudojo ID failus ir sertifikatus vartotojų bei serverių identifikavimui. Saugumas jau palaikomas vartotojo identifikacijos nustatyme, bei prieiga prie duomenų nurodoma serverio, duomenų bazės, view'o bei lauko lygyje. Viešojo rakto naudojimas leido naudotis laiškų pasirašymą bei kodavimą.

Pirmos versijos saugumo savybės:

- Vartotojų ID failai, apsaugoti slaptažodžiais.
- Vieši ir privatūs raktai.
- Sertifikatai.
- Pašto kodavimas ir pasirašymas.
- ACL'as bei rolės ir privilegijos.
- Portų kodavimas.

1.2.1991: Versija 2.0

Antroje versijoje buvo kodavimo technologijos vystytos, ko pasekoje atsirado simetrinio rakto naudojimas. Galima išskirti du punktus:

- Dokumentų kodavimas
- Slapti kodavimo raktai.

1.3.1993: Versija 3.0

Kadangi Notes pradėti naudoti didelėse organizacijose, pagerinti Notes viešojo rakto valdymą, buvo įvesti hierarchiniai sertifikatai. Taip pat prieiga nuleista iki dokumentų lygio.

Pagrindinės savybės:

- Hierarchiniai sertifikatai.
- Rolės
- Reader Names/Author Names laukai

- Skaityti bei kurti vartotojų sąrašai (Read and Compose Access Lists)

1.4.1996: Versija 4.0

Saugumas vystėsi apsaugant lokalias DB kopijas bei pagerinant ID failų saugumą.

Naujos saugumo savybės:

- Lokalių DB kodavimas.
- DB dizaino kodavimas
- ID slaptažodžio spėjimo apsunkinimas
- Anonymous vartotojų (neautorizuotų WEB vartotojų) prieiga.

1.5.1996: Notes ir Domino versija 4.5

Didžiausia naujovė – vykdymo kontrolės sąrašai (Execution Control Lists (ECL)) buvo įgyvendinti, norint apsaugoti darbo vietas nuo nežinomo kodo vykdymo. Tam, kad tai galima būtų įgyvendinti, visų dizaino elementų pasirašymas tapo būtinybe.

Svarbiausios savybės:

- SSL (Secure Sockets Layer) 2.0 palaikymas Notes klientui ir Domino serveriui.
- Execution Control Lists (ECLs)
- Slaptažodžio keitimas ir ID rakinimas
- Slaptažodžio galiojimo laikas

1.6.1999: Notes ir Domino versija 5.0

Su R5, saugumas vystėsi toliau, įtraukdamas pasaulinių technologijų pasikeitimus ir patobulinimus, leidžiančius lengviau administruoti didžiules, po visą pasaulį išsibarsčiusias korporacijas. R5 versijoje buvo įvesta WEB autentikacija, palaikanti sesijas. Sesijomis grindžiama autentikacija yra realizuota naudojant cookies (sausainiukus) ir palaiko sesijų galiojimo intervalus bei suteikia konfigūruojamas vartotojo įsiloginimo formas.
SSLv3 palaikymas buvo išplėstas ne tik HTTP protokolui, bet ir į kutus protokolus, kuriuos palaiko Domino: LDAP, POP3, IMAP, NNTP ir IIOP. S/MIMEv2 palaikymas buvo realizuotas Notes kliente, įgalinantis pašto pasirašymą ir kodavimą siunčiant

laiškus ir už Notes pašto ribų. Slaptažodžio kokybė pakeitė slaptažodžio ilgumo reikalavimus. Kai vartotojai užmiršta slaptažodį, buvo pridėta funkcija administratoriams, notes ID atstatymui.

Naujos saugumo savybės:

- S/MIME
- SSLv3 visiems Internet'o protokolams.
- ID ir slaptažodžių atstatymas Notes vartotojams.
- Slaptažodžių kokybė.
- Sesijomis grįsta Web autentikacija.

2. Saugumas

Lotus Notes/Domino saugumo sąvoka yra labai svarbi ir yra viena iš pagrindinių Domino išskirtinumo bruožų. Lotus Notes/Domino saugumas yra skirstomas į šiuos lygius, pagal prieigos suteikimo teises:

1. Serverio lygis
2. Duomenų bazės lygis
3. Dokumento lygis
4. Lauko lygis

Taip pat, Notes/Domino saugumas yra užtikrinamas ne tik prieigos teisėmis, tačiau ir pasirašymo bei duomenų kodavimo funkcijomis.

3. Serverio prieigos lygis

Autentikacija

Serverio įrašo laukai (kas ką gali atlikti: prisijungti prie serverio, naudotis serveriu kaip proxy, kurti naujas DB, naujas DB replikas, ….)

4. Duomenų bazės prieigos lygis

Prieigos teises prie duomenų bazės yra nusakomos taip vadinamu *Access Control List (ACL)* – Kontroliuojamos Prieigos Sąrašas.

Kiekvienos DB ACL yra pasiekiamas per *File->Database->Access Control…* meniu punktą – tuomet vartotojui pateikiamas ACL'o konfigūravimo langas, kuris susideda iš 4 panelių.

4.1."Basics" panelė

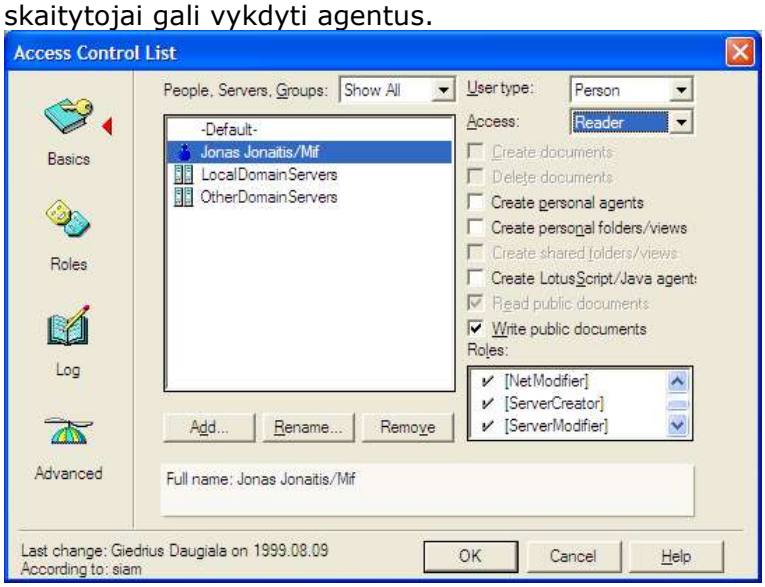
No Access

No Access reiškia nėra jokių galimybių prieigai. Jokios prieigos.

Depositor

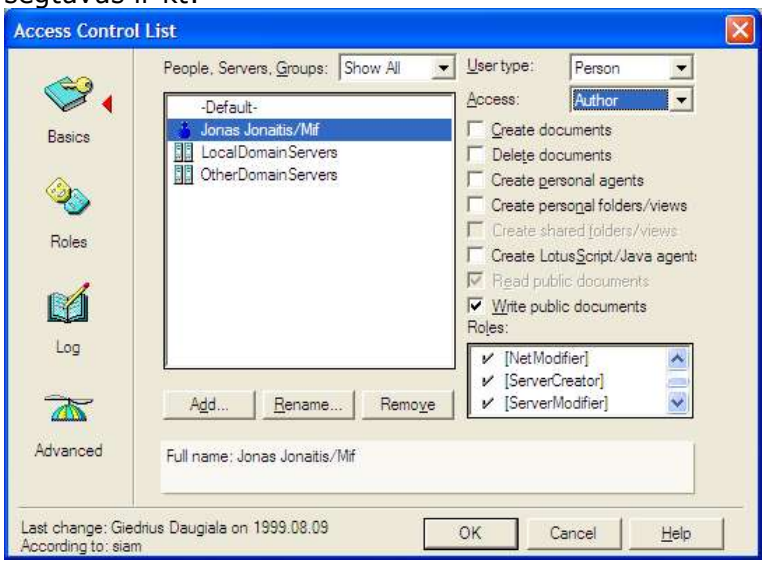
Depositoriai gali tik kurti naujus dokumentus į DB, bet jie negali perskaityti ir tuo pačiu redaguoti visų DB esančių dokumentų.

Reader
Reader (skaitytojai) gali skaityti dokumentus, bet negali jų kurti. Tačiau, skaitytojai gali vykdyti agentus.



Authors
Autoriai turi visas skaitytojų teises bei dar autoriai gali kurti bei redaguoti savo dokumentus ("Savo" – tai reiškia, kad "Authors" tipo lauke dokumente yra paminėtas autoriaus vardas). Reikia pabrėžti, kad galima redaguoti tik tuos dokumentus, kuriems vartotojas yra autorius – t.y. jis "įeina" į Authors tipo lauką dokumente (gali būti įvardintas tiesiogiai, per rolę, per grupę).

Čia galimos jau įdomios papildomų teisių suteikimo galimybės. T.y. trinti dokumentus, kurti dokumentus, kurti asmeninius agentus, kurti asmeninius segtuvus ir kt:



Editors
Editoriai turi visas autorių teises bei gali kurti bei redaguoti visus dokumentus.

Editoriai gali gauti galimybes kurti personalinius agentus, personalinius vaizdinius bei segtuvus, kurti bendrus vaizdinius segtuvus, taip pat kurti LotusScript ar Java agentus.

Designers
Designer teises turintys vartotojai turi tas pačias teises, kaip ir Editors, tačiau jie gali modifikuoti dizainą, DB savybes, kurti pilnatekstį indeksą. Tačiau, nuo jų galima atšaukti teises kurti LotusScript bei Java agentus ir trinti dokumentus.

Managers
Managers turi galimybę atlikti viską – t.y. viską, ką gali daryti dizaineris plius modifikuoti (valdyti) DB ACL'ą. Jiems galima tik uždrausti trinti dokumentus – tačiau tą teisę jie patys gali sau ir susiteikti.

Vartotojų tipai

Kiekvienas vartotojas gali turėti savo tipą. Jei kartais vartotojo vardas, kai jis kreipiasi į DB, atitinką vardą, nurodytą ACL'e, tai dar yra tikrinama, ar vartotojo tipas atitinką nurodytą vardui tipą ir tik tuo atveju vartotojas gauna prieigą prie DB. Yra šie vartotojų tipai:

- **Person** tai vartotojai.
- **Person Group** – vartotojų grupės
- **Server** - serveris.
- **Server Group** Serverių grupė.
- **Mixed Group** – mišri grupė.

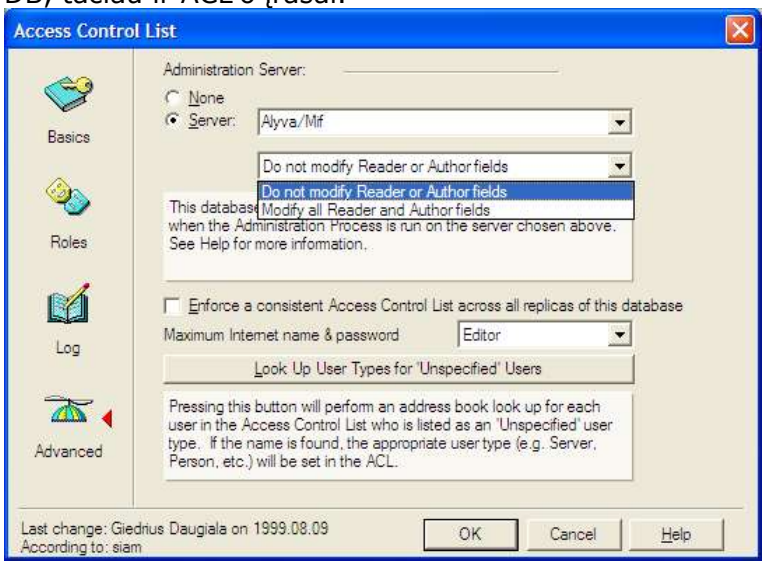
Rolės
Rolės leidžia detaliau skirstyti vartotojus į grupes tik DB ribose, jas kuriant ir suteikiant DB manager teises turinčiam vartotojui. Tai leidžia lanksčiau naudotis teisių suteikimo sistema, nei vartotojų grupės.

Log panelė
ACL'o pakeitimai yra fiksuojami ir žurnalizuojami. Visi visų vartotojų bei serverių ACL'o keitimai yra protokoluojami ("loginami").

Advanced panelė
Joje galima nurodyti DB ACL'o administravimo serverį. Administravimo serveris – tai tas serveris, kuris atlieka visus ACL'o pakeitimus, kai keičiasi (vykdant

funkcijas *rename* arba *recertificate*) vartotojų vardai. Taip pat, jei dar tam serveriui nurodyta, jis gali vartotojo vardų pasikeitimus "nustumti" ne tik į ACL'ą, bet ir į visus DB saugomų dokumentų *Reader* arba *Author* laukus.

Taip pat, labai svarbus punktas – nurodoma, ar ši DB turi išlaikyti vientisą replikos ACL'ą su kitomis DB ar ne. Jei požymis yra užžymėtas, tai reikš, kad kiekvieno replikavimo metu bus sinchronizuojami ne tik duomenys tarp skirtingų DB, tačiau ir ACL'o įrašai.



Taip pat, reikėtų pastebėti, kad duomenų bazėje, saugomoje lokaliai, ACL'o nustatymai galioja tik tuo atveju, jei minėtas požymis "Enforce a concistent Access Control List across all replicas of this database" yra pažymėtas. Priešingu atveju, visi vartotojai turės manager teises bei rolių nustatymai negalios.

5. View'o ir formos teisės

View'ams (segtuvams ir virtualiems segtuvams) galima nurodyti, kokie vartotojai, vartotojų grupės arba vartotojai, turintys nurodytas roles, gali peržiūrėti segtuvo turinį.

Form'oms taip pat galima nurodyti, kokie vartotojai, jų grupės ir rolės pagal nutylėjimą turi būti skaitytojai sukurtų dokumentų (pagal nutylėjimą yra saugoma "visi"). Nurodyti vartotojai yra išsaugomi prie dokumentų, sukurtų su forma, lauke vardu "$Readers".

Taip pat, prie formų galima išsaugoti, kokie vartotojai, jų grupės bei rolės gali kurti dokumentus su forma.

Dar vienas formos požymis – "Disable printing/forwarding/copying to clipboard" – jo pažymėjimas reiškia, kad dokumentų, sukurtų su tokia forma, negalima bus atspausdinti, kopijuoti turinio į laikiną atmintį, persiųsti laišku:

6. Authors Readers laukai

Prieigai dokumento lygyje valdyti yra naudojami Auhors ir Readers tipo laukai dokumente.

Skaitymo (matomumo) prieigai valdyti yra naudojami Readers tipo laukai. Jei dokumente egzistuoja bent vienas netuščias Readers tipo laukas, tai tą dokumentą galės matyti tik tie vartotojai, kurie tenkins bent vieną iš sekančių sąlygų:

- Vartotojo vardas yra paminėtas bent viename Readers tipo lauke.
- Bet kurios grupės, kuriai priklauso vartotojas, vardas yra paminėtas bent viename Readers tipo lauke.
- Bet kurios rolės, kurią turi vartotojas, pavadinimas yra paminėtas bent viename Readers tipo lauke.
- Vartotojas turi teises į dokumentą per kurį nors Authors tipo lauką.

Dokumentą galės skaityti visi vartotojai su didesnėmis nei Depositor teisėmis, jei:

- Dokumente nėra nei vieno Readers tipo lauko
- Visi Readers tipo laukai yra tušti
- Bent viename Readers tipo lauke yra reikšmė "*".

Apribojimas pagal Readers tipo laukus yra taikomas visiems vartotojams, nepriklausomai nuo jų teisių, įgyjamų per ACL'ą, t.y. net Manager teises turintys vartotojai nematys dokumento, jei taip bus nurodyta naudojant readers tipo laukuose dokumente.

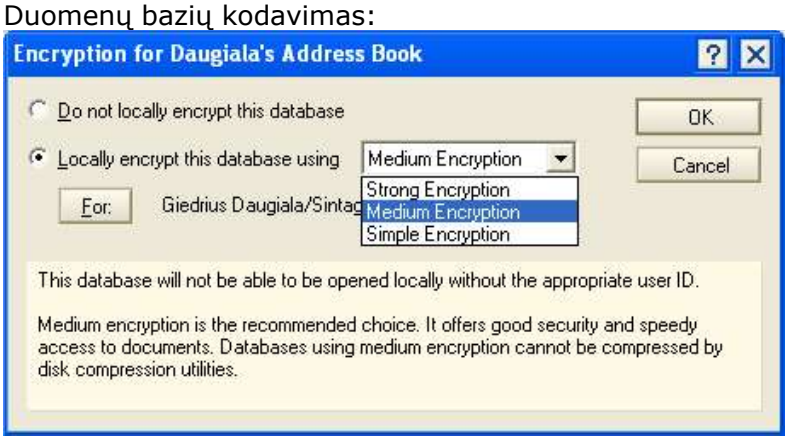
Authors tipo laukai naudojami nurodyti dokumento redagavimo teises Author teises turintiems vartotojams (visiems kitiems vartotojams (Readers, Editors, it kt.) Author tipo laukai nei suteikia, nei prideda teisių redaguoti dokumentą). Taigi, Author teises turinti vartotojas galės redaguoti dokumentą tik tada, jei:

- Vartotojo vardas yra paminėtas bent viename Authors tipo lauke.
- Bet kurios grupės, kuriai priklauso vartotojas, vardas yra paminėtas bent viename Authors tipo lauke.
- Bet kurios rolės, kurią turi vartotojas, pavadinimas yra paminėtas bent viename Authors tipo lauke.
- Bent viename Authors tipo lauke yra simbolis "*".

7. Kodavimas ir pasirašymas

Duomenų bazės, dokumentų laukai bei laiškai gali būti koduojami.

Duomenų bazių kodavimas:



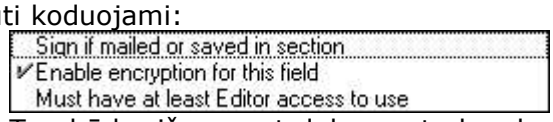
Duomenų bazės gali būti koduojamos, naudojant vartotojo (taip pat serverio) ID. Užkodavus duomenų bazę su nurodytu ID, ją galima bus atidaryti tik naudojant tą ID. Yra galimi trys kodavimo lygiai:

- Stiprus
- Vidutinis
- Paprastas

Užkodavus DB, gali sulėtėti darbas su ja, segtuvų atidarymas ir pan. Rekomenduojama naudoti vidutinį kodavimo lygį – jis pakankamai saugus ir gana greitas.

Dokumentų kodavimas:

Tarp visų laukų dokumente, kai kuriuos laukus galima nurodyti, kad jie turi būti koduojami:



Tuo būdu, išsaugant dokumentą bus koduojami laukai užkuodoti su raktu, kuris gali būti nurodytas vienu iš sekančių būdų:

- Programiškai
- Vartotojo interaktyviai
- Formos kodavimo raktas pagal nutylėjimą.

Norint koduoti dokumento laukus, arba užkuoduotus perkaityti, vartotojas turi turėti savo ID faile taip vadinamą kodavimo raktą, kurį sukuria ir platina administratorius arba sistemos architektas (designer'is)

Siunčiami laiškai yra koduojami naudojant asimetrinį kodavimą – su gavėjo viešu raktu. Laišką galima atkoduoti tik naudojant gavėjo privatų raktą, kuris yra saugomas gavėjo ID faile.

Pasirašyme atvirkščiai – laiške dalis informacijos, pagal kurią galima nustatyti, pasikeitė laiškas ar ne, yra užkoduojama naudojant privatų siuntėjo raktą, ir tą informaciją galima dekoduoti naudojant viešą siuntėjo raktą.