2003－DSM－30　(5)
2003／9／26

階層型VPNにおける効率的なアクセスポリシ管理手法

福井 健太†　岡山 聖彦††　山井 成良†††　石橋 勇人‡　松浦 敏雄‡

概　要

VPNドメインが階層的に構成されたネットワークでは，アクセスポリシ (認証および暗号化通信の有無やその方法等)が通信先のVPNドメイン毎に異なるので，あるVPNドメインにおいて，下位VPNドメイン毎に異なるアクセスポリシを設定しなければならない場合がある．しかし，従来のVPN技術では，アクセスポリシを各VPNゲートウェイが保持する静的な設定ファイルに記述するため，あるVPNドメインの管理者は下位VPNドメインの管理者と協調してアクセスポリシを設定する必要がある．このため，組織の内部構造が複雑になるにつれて，アクセスポリシ管理の手間が増大するという問題がある．そこで本論文では，このような問題を解決するための効率的なアクセスポリシ管理手法を提案する．提案法では，アクセスポリシを階層的に表現すると共に，自動的にアクセスポリシを下位VPNドメインに問い合わせる機能を持つポリシサーバを各VPNドメインに導入することで，アクセスポリシ管理の手間を軽減している．提案法の有効性は，提案法に基づいて実装したポリシサーバを用いて実施した性能評価実験によって確認している．

A Efficient Management Method of Access Policies for Hierarchical Virtual Private Networks

Kenta Fukui†　Kiyohiko Okayama††　Nariyoshi Yamai†††
Hayato Ishibashi‡　Toshio Matsuura‡

Abstract

In Virtual Private Networks(VPNs) having hierarchical structure, since each VPN domain has different access policy (whether VPN gateway should perform authentication and data encryption, and so on), the administrator of a VPN domain may need to configure access policies which are different from every VPN subdomain. However, in the existing VPN methods, since access policies are stored in static configuration file of each VPN gateway, the administrator of a VPN domain has to cooperate with the other administrators of its subdomains. Therefore, management cost of access policies becomes fairly large if the organization has complicated structure. In this paper, we propose an efficient management method of access policies for hierarchical VPN. To reduce management cost, we introduce a database with hierarchical structure to represent access policies easily and policy servers to get access policies automatically. The effectiveness of our method is confirmed by the experiment on the actual network using policy servers based on our method.

†岡山大学大学院自然科学研究科, Graduate School of Natural Science and Technology, Okayama University
††岡山大学工学部, Faculty of Engineering, Okayama University
†††岡山大学総合情報処理センター, Computer Center, Okayama University
‡大阪市立大学大学院創造都市研究科, Graduate School of Creative Cities, Osaka City University

1 はじめに

インターネットを介して自組織のネットワークに安全にアクセスするための技術として，仮想プライベートネットワーク (Virtual Private Network，以下VPNという)が注目されている．VPNにはさまざまな実現方法があるが，ホスト–ホスト間でVPNリンクを構成するものと，ホスト–ネットワーク間(あるいはネットワーク–ネットワーク間)でVPNリンクを構成するものに分けられる．前者はVPNを利用するアプリケーションクライアントとサーバの両方にVPNのためのソフトウェアを組み込まなければならないのに対し，後者の多くはアプリケーションサーバへの組み込みを必要としないので，本論文では後者のVPN実現方法を対象とする．

このようなVPNでは，組織内など同一のアクセスポリシを持つ範囲をVPNドメインと呼び，VPNドメインを跨る通信を制御するVPNゲートウェイ(以下VGWという)を設置する．ここでアクセスポリシとは，接続元および接続先ホストの情報等に基づくアクセス制御の方針であり，認証および暗号化通信の有無や方法，アクセスの可否等などが含まれる．このとき，大規模な組織ではアクセスポリシが部署ごとに異なる場合が多いので，VPNドメインをインターネットのドメインと同様に階層的に構成するのが自然である (以下，階層型VPNという)．このような構成において，組織外にあるクライアントが組織の最も内側のVPNドメインにアクセスするには，最も外側のVPNドメインから内側に向かって1つずつVGWを辿る必要がある．

階層型VPNに対応可能な既存のVPNリンク確立方式として，SOCKS Version 5[1]プロトコルの参照実装であるSOCKS5[2]の多段プロキシ機構を利用する方式や，仮想パスを用いた方式[3] (以下，これらをまとめて従来法という)などがある．従来法はいずれも，複数のVGWを自動的に辿る機能を持つが，アクセスポリシを各VGWが保持する静的な設定ファイルで管理するので，各VGWで下位のVPNドメイン毎に異なるアクセスポリシを設定するためには，上位のVPNドメインの管理者は，予め組織の内部構成を把握すると共に，必要であれば下位VPNドメインの管理者から自ドメインで設定すべきアクセスポリシ (以下，アクセスポリシ要求という) を聞いた上で設定ファイルに記述する必要がある．このため，内部構成が複雑になるにつれて，アクセスポリシ管理の手間が増大するという問題がある．

本論文では，上述した問題を解決するための，効率的なアクセスポリシ管理手法を提案する．提案法では，文献[4]の経路制御手法で用いられているLDAPサーバのディレクトリデータベースを利用して，下位のVPNドメイン毎に異なるアクセスポリシを階層的に表現すると共に，下位VPNドメインのアクセスポリシ要求を自動的に問い合わせる機能を持つポリシサーバを各VPNドメインに導入する．これにより，自VPNドメインにおけるアクセスポリシの決定権を下位のVPNドメインに委譲することが可能となるので，各VPNドメインの管理者は，下位のVPNドメイン構成やアクセスポリシ要求を事前に把握する必要がなくなる．

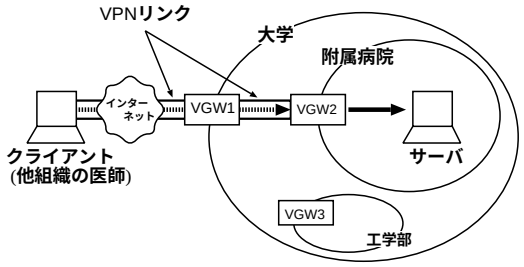

図 1: 階層型VPN

以下，従来法の問題点を考察した後，提案法の概要について述べ，その有効性を確かめるために実施した性能評価実験について述べる．なお，文献[4]の経路制御手法と同様に，本論文においても，原則としてVPNドメインをDNSのドメインと一致させることを前提とする．以下，特に明記しない限り，ドメインという用語はVPNドメインとそれに対応するDNSドメインの両方を指すものとする．

2 従来法の問題点の考察

1で述べたように，階層型VPNではドメイン毎にアクセスポリシが異なるので，場合によってはアクセスを中継する下位ドメイン毎に異なるアクセスポリシを設定する必要がある．例えば，図1のようなドメイン構成において，大学全体のドメインに設置されたVGW1では，大学外にあるクライアントが内部にアクセスする場合には認証を行うものとする．このとき，附属病院のドメインにおいて，他組織の医師に対してこのドメイン内にあるサーバへのアクセスを許可しようとすると，VGW1とVGW2の両方にアカウントを登録するか，あるいは，外部から附属病院ドメインにアクセスする際にはVGW2でのみ認証を行い，VGW1では認証しないように設定する必要がある．後者の場合，VGW1では,「中継先が附属病院ドメインの場合には認証

を行わない」という設定を施さなければならない．

従来法においてこのような状況に対応する場合，アクセスポリシを各VGWの設定ファイルで保持し，接続元および接続先の組と，それに対応するアクセスポリシのルールを記述すればよい．接続元および接続先には，ホスト名やIPアドレスの他，ドメイン名やネットワークアドレスを指定することができるが，簡単化のため，以降ではアクセスポリシを認証の有無のみとし，接続先のドメイン名のみに基づいてアクセスポリシを決定するものとする．

ところが，従来法において下位ドメイン毎に異なるアクセスポリシを設定しようとすると，上位ドメインの管理者は，VGWの設定ファイルに接続先のドメイン名と対応するアクセスポリシを列挙することになる．したがって，上位ドメインの管理者は予め組織の内部構造(自ドメインより下位のドメイン構成)と下位ドメインのアクセスポリシ要求を把握した上で，各VGWの設定ファイルに手作業で登録しなければならない．そのため，各ドメインの管理者間で調整が必要となり，特に内部構造が複雑な組織において，アクセスポリシ要求が下位ドメイン毎に異なる場合には，上位ドメインにおけるアクセスポリシ管理の手間が大きくなるという問題がある．

3　アクセスポリシ管理手法の提案

2で述べた問題は，自ドメインに対する下位ドメインからのアクセスポリシ要求を，事前に把握して自ドメインの設定ファイルに記述しなければならないことに起因する．したがって，下位ドメインにアクセスを中継する際のアクセスポリシの決定権を必要に応じて下位ドメインに委譲し，上位ドメインではアクセスの発生時に自動的に下位ドメインにアクセスポリシを問い合わせるようにすれば，この問題を解決できると考えられる．

以下，アクセスポリシ決定権の委譲と自動問合せを実現するための，アクセスポリシの階層的表現方法とポリシサーバについて述べた後，提案法によるVPNリンク確立手順について述べる．

3.1　アクセスポリシの階層的表現

階層型VPNでは，ドメインが階層的に構成されるので，下位ドメイン毎に異なるアクセスポリシを効率よく表現するために，提案法では，文献[4]の経路制御手法で用いられているLDAPサーバのディレクトリデータベース(以下，データベースという)を利用することにする．

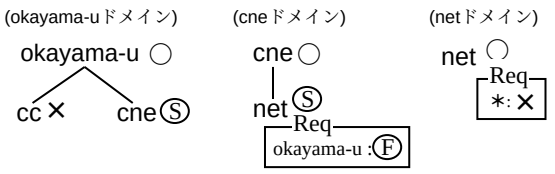

図 2: データベースの例

まず，各ドメインに設置されたLDAPサーバのデータベースでは，自ドメインを根とする木構造を形成し，必要に応じて下位ドメインを木のノードに割り当てた上で，ノードの属性としてアクセスポリシを登録する．そして，アクセス制御の際には，VGWはLDAPサーバに対して接続先のドメイン名をキーとして問合せを行い，LDAPサーバでは，データベースを検索することにより，最も長くマッチするドメインのノードに登録されたアクセスポリシを返すものとする．なお，マッチしたドメインのノードにアクセスポリシが定義されていない場合には，上位ドメインのノードに登録されたアクセスポリシが適用されるものとする．

一方，特定の下位ドメインに対してアクセスポリシの決定権を委譲するために，ノードに登録する属性として，探索フラグ，中継フラグ，および，アクセスポリシ要求の3つを追加する．

探索フラグは，自ドメインでのアクセスポリシの決定を下位ドメインに委ねることを意味し，このフラグが設定されていた場合には，対応する下位ドメインにアクセスポリシの問合せを行うものとする．アクセスポリシ要求には，問合せの起点となる(上位の)ドメイン名と，それに対して返すべきアクセスポリシの値の組を登録する．これにより，問合せを行う上位ドメインに応じて異なるアクセスポリシを返すことが可能となる．中継フラグは，上位ドメインからの問合せをさらに下位のドメインに中継するための属性であり，問合せを行う上位ドメインに応じて中継するか否かを変更できるよう，アクセスポリシ要求の属性値として登録する．

図2にデータベースの例を示す．図の左から順に，組織全体を表すokayama-uドメインとその直下にあるcneドメイン，さらに下位にあるnetドメインの各LDAPサーバが保持しているデータベースを示している．図中において，“○”は認証あり，“×”は認証なしを意味し，“S”は探索フラグ，“F”は中継フラグ，“Req”はアクセスポリシ要求をそれぞれ意味する．

図2の各データベースは，接続先のドメイン名をキーとして検索され，okayama-uドメインのLDAPサーバを検索する際，検索キーがcc.okayama-

u.ac.jp(あるいはそのサブドメイン)であれば，ノード ccにマッチして「認証なし」が適用される．これは，okayama-uドメインのVGWでは認証を行わないことを意味する．また，検索キーにccあるいはcne以外のドメインが指定された場合には，すべてノード okayama-uにマッチし「認証あり」が適用される．このように，上位ドメインと同様のアクセスポリシを適用する場合には，下位ドメインに対応するノードを登録しないことによってデータベースを小さくすることができる．

一方，検索キーがnet.cne.okayama-u.ac.jpの場合には，ノード cneにマッチするが，属性として探索フラグ(S)が設定されているため，cneドメインにアクセスポリシを問い合わせなければならないことがわかる．次に，okayama-uドメインからcneドメインのLDAPサーバに対して，net.cne.okayama-u.ac.jpをキーとした問合せがあると，ノード netにマッチし，そこに登録されたアクセスポリシ要求(Req)が適用される．この例では，アクセスポリシ要求の属性値として中継フラグ(F)が設定されているので，okayama-uドメインからの問合せを，さらにnetドメインに中継しなければならないことがわかる．最後に，okayama-uドメインからの問合せを受けたnetドメインでは，検索の結果，ノード netに登録されたアクセスポリシ要求が適用される．この例では，アクセスポリシ要求のドメイン名の部分にワイルドカード(*)が指定されており，すべての問合せに対して「認証なし」を応答する．したがって，okayama-uドメインのVGWでは，接続先がnet.cne.okayama-u.ac.jpドメインの場合は，認証を行わないことになる．

なお，組織のネットワークを外部から護るという観点から，外部に近い上位ドメインが，下位ドメインよりも強い権限を持つ必要があると考えられる．このため，データベースのノードに通常のアクセスポリシの属性値(認証の有無)と探索フラグの両方が登録された場合には，前者を優先する．これは，下位ドメインにアクセスポリシの決定権を委譲している場合でも，上位ドメインによってその内容が上書きできることを意味する．

3.2 アクセスポリシ自動問合せ機能

3.2.1 ポリシサーバの導入

3.1で述べたデータベースに基づいて，アクセスポリシの検索や下位ドメインに対する問合せあるいは中継を行うために，提案法では，ポリシサーバを導入する．ポリシサーバは，各ドメインに設置し，同じドメインのVGWからの要求を受けてLDAPサーバを検索し，結果として得られたアクセスポリシをVGWに返す．このとき，アクセスポリシとして探索フラグが得られた場合には，自動的に下位ドメインのポリシサーバに問合せを行う．

一方，上位ドメインからの問合せを受けたポリシサーバは，自ドメインのLDAPサーバを検索し，アクセスポリシ要求が得られればそれを上位ドメインのポリシサーバに返す．このとき，アクセスポリシ要求の属性値として中継フラグを取得した場合には，さらに下位のポリシサーバに問合せを中継し，その結果を上位ドメインのポリシサーバに返す．

3.2.2 キャッシュ機能と一括問合せ機能

3.2.1で述べたポリシサーバの導入により，上位ドメインにおいて事前に下位ドメインからのアクセスポリシ要求を把握する必要はなくなるが，アクセスポリシの問合せに伴う通信が発生するため，データベースの設定によってはオーバーヘッドが大きくなることが予想される．特に，組織外のクライアントから接続先のドメインに至るまでのすべての上位ドメインにおいて，アクセスポリシの問合せが接続先，すなわち，最下位ドメインのポリシサーバへ中継されるように設定されている場合，クライアントが途中のVGWに接続する度に，接続先ドメインのポリシサーバまで問合せが発生することになる．

そこで提案法では，ポリシサーバにキャッシュ機能と一括問合せ機能を追加する．あるドメインのポリシサーバに対して，上位ドメインから問合せがあった場合，LDAPサーバの検索結果として中継フラグと探索フラグとの両方が得られた場合には，必ずそのドメインのポリシサーバを起点とする問合せが生じることは明らかである．そこで，上位ドメインからの問合せを中継する際のメッセージに，自らを起点とする問合せのメッセージを多重化して送信し，その結果得られた自ドメインに対するアクセスポリシ要求をキャッシュしておけば，クライアントが自ドメインのVGWに接続した際には，下位ドメインに対して問合せを行うことなくアクセスポリシを決定することができる．

なお，ポリシサーバにおけるアクセスポリシのキャッシュは，一括問合せ時だけでなく，ポリシサーバが自ドメインのLDAPサーバを検索する際にも行う．これにより，同一接続先に対する2回目以降のアクセス時には，LDAPサーバの検索を行う必要がないので，アクセスポリシの決定に伴って生じる通信のオーバーヘッドを大幅に削減できると考えられる．

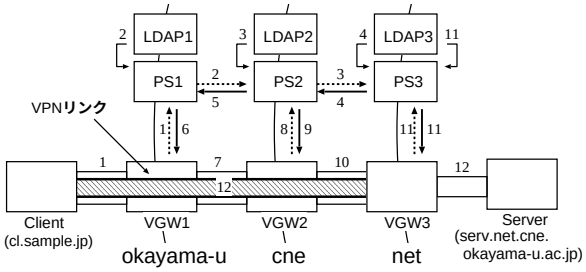

図 3: 提案法による VPN リンク確立例

3.3 VPNリンク確立手順

提案法を文献 [4] の VPN リンク確立方式に適用した場合の，VPN リンク確立手順の例を図3に示す．図3において，組織のドメイン (okayama-u) の下位に cne ドメイン，さらにその下位に net ドメインが設置されている．各ドメインには，VGW，ポリシサーバ (PS)，LDAP サーバ (LDAP) が設置されているものとする．一方，各 LDAP サーバのデータベースは，図2のように設定されているものとする．この例では，すべての上位ドメイン (okayama-u および cne) において，接続先のドメインまでアクセスポリシの問合せが行われる．

このような構成において，組織外のクライアント (cl.sample.jp) が net ドメイン内のサーバ (serv.net.cne.okayama-u.ac.jp) にアクセスする手順を以下に示す．

1. クライアントは VGW1 に対しコネクションを確立すると，VGW1 は PS1 にアクセスポリシを問い合わせる．
2. PS1 は通信先のサーバの FQDN を用いて LDAP1 を検索すると，データベースのノード cne にマッチする．このノードには探索フラグが登録されているので，PS2 にアクセスポリシを問い合わせる．
3. PS2 は通信先のサーバの FQDN を用いて LDAP2 を検索すると，データベースのノード net にマッチし，okayama-u へのアクセスポリシ要求として中継フラグを取得する．この例では，ノード net に登録された探索フラグも得られるので，PS2 は okayama-u ドメインからの問合せの中継と，cne ドメインを起点とする問合せを，PS3 に対して一括して行う．
4. PS3 は LDAP3 から okayama-u ドメインと cne ドメインに対するアクセスポリシ要求を検索すると，いずれもデータベースのノード net に登録されたアクセスポリシ要求 (認証なし) にマッチするので，結果を PS2 に返す．
5. PS2 は，自ドメイン (cne) に対するアクセスポリシ要求をキャッシュすると共に，okayama-u ドメインに対するへのアクセスポリシ要求を PS1 に返す．
6. PS1 は，自ドメイン (okayama-u) に対するアクセスポリシ要求をキャッシュすると共に，そのアクセスポリシを VGW1 に返す．
7. VGW1 は取得したアクセスポリシ (認証なし) に従い，認証は行わず，クライアント-VGW1 間で確立されたコネクションを仮想パスとする．さらに，VGW1 は VGW2 に対してコネクションを確立し，以降パケットを透過的に転送する．
8. VGW2 は PS2 にアクセスポリシを問い合わせる．
9. PS2 は一括問合せで取得したアクセスポリシのキャッシュがあるので，それを VGW2 に返す．
10. VGW2 は取得したアクセスポリシ (認証なし) に従い，認証は行わず，VGW1-VGW2 間で確立されたコネクションを仮想パスとする．さらに，VGW2 は VGW3 に対しコネクションを確立し，以降パケットを透過的に転送する．
11. VGW3，PS3 も同様に動作し，アクセスポリシとして「認証あり」を得るので，クライアントと認証を行う．認証に成功すると，VGW2-VGW3 間で確立されたコネクションを仮想パスとする．
12. VGW3 は，クライアントとの間で VPN リンクを確立すると共に，接続先のサーバとコネクションを確立し，以降パケットを転送する．これにより，クライアント-サーバ間での通信が可能となる．

4 性能評価

提案法では，LDAP サーバの検索や下位ドメインに対するアクセスポリシの問合せの際に通信が生じるので，従来法と比べて VPN リンク確立時のオーバヘッドがどの程度増加するかを調べるために，性能評価実験を行った．実験には，文献 [4] の実装に対して，3で述べたポリシサーバを追加すると共に，ポリシサーバへのアクセス機能を組み込んだ VGW を利用した．また，VPN リンク確立時の認証については，SOCKS5 がサポートする Kerberos Version 5 GSS-API Mechanism[6] を用いている．

実験ネットワークの構成を図4に示す．一括問合せを行うためにドメインの階層数は3とし，各ドメインに VGW，ポリシサーバ，LDAP サーバを配置

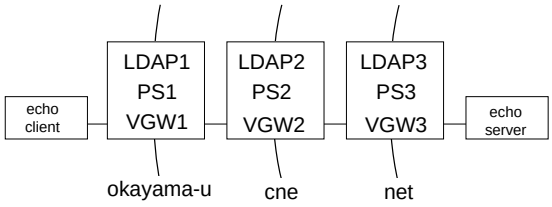

図 4: 実験ネットワークの構成

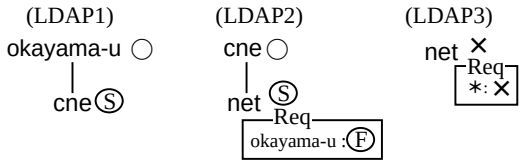

図 5: 各LDAPサーバのデータベース (認証なし)

している．なお，実験に利用した各計算機は学内ネットワークを利用して，10Mbps または 100Mbps のリンクにより接続した．

実験は，文献 [4] の方式 (従来法) と，提案法においてキャッシュがある場合 (方法1)，キャッシュがなく一括問合せを行う場合 (方法2)，キャッシュがなく一括問合せを行わない場合 (方法3) の4通りについて，それぞれ，すべての VGW で認証を行わない場合 (図5) とすべての VGW で認証を行う場合 (図6) の2通りを組み合わせ，すべての組合せ (8通り) について，組織外にある echo クライアントが，組織の最も内側のドメインにある echo サーバに対してコネクションを確立する試行を 100 回行い，コネクション確立に要した時間の平均値を算出した．

表1に実験結果を示す．従来法と (提案法において最も時間がかかる) 方法3の差は約 170ms であるが，一度 VPN リンクが確立すると，経路上のすべてのポリシサーバにキャッシュができるので，表1の方法1からわかるように，2回目以降の VPN リンク確立に要する時間は従来法に比べて約 20ms しか増加しない．また，認証ありの場合はいずれも約 1300ms 以上かかるので，提案法による VPN リンク確立時間の増加は実用上問題ないと考えられる．また，方法2と方法3の比較によって，一括問合せの有効性が確認できる．本実験ではその差は約 10ms であるが，一括問合せの有効性は，階層数が増えるにつれて大きくなると考えられる．

5 おわりに

本論文では，階層型 VPN における従来のアクセスポリシ管理手法を考察し，その問題点を解決するための効率的なアクセスポリシ管理手法を提案した．さらに，提案法に基づいて既存の VGW の拡張

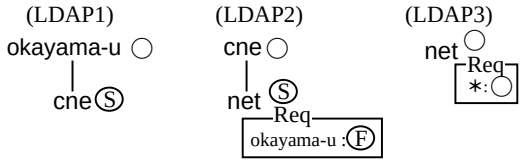

図 6: 各LDAPサーバのデータベース (認証あり)

表 1: 実験結果

	コネクション確立時間 (ms)	
	認証なし	認証あり
従来法	64	1313
方法1	84	1330
方法2	231	1479
方法3	245	1487

とポリシサーバの実装を行い，これらを用いた性能評価実験を行うことによって，提案法の有効性を確認した．

今後の課題としては，ユーザのグループ単位でのアクセス制御や認証方法の多様化などといった，さらなる柔軟性の向上が挙げられる．

参考文献

[1] Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D. and Jones, L.: *SOCKS Protocol Version 5*, RFC1928 (1996).

[2] NEC: *SOCKS Home Page*, http://www.socks.nec.com/index.html.

[3] 岡山聖彦, 山井成良, 石橋勇人, 安倍広多, 松浦敏雄: 代理ゲートウェイを用いたSOCKSベースの階層的VPN構成法, 情報処理学会論文誌, Vol.42, No.12, pp.2860–2868 (2001).

[4] 岡山聖彦, 金出地友治, 山井成良, 石橋勇人, 松浦敏雄: 階層型VPNのためのLDAPサーバを用いた経路制御手法, 情報処理学会研究報告, 2003-DSM-29, pp.57–62 (2003-04).

[5] M. Wahl, T. Howes, S.Kille.: *Lightweight Directory Access Protocol (v3)*, RFC 2251 (1997).

[6] Kohl, J. and Neuman, C.: *The Kerberos Network Authentication Service (V5)*, RFC1510 (1993).

[7] A.Gulbrandsen, P. Vixie, L. Esibov.: *A DNS RR for specifying the location of services (DNS SRV)*, RFC 2782 (2000).

[8] Linn, J.: The Kerberos Version 5 GSS-API Mechanism, RFC 1964 (1996)