



F5 Technical Brief

Kerberos Constrained Delegation and Protocol Transition in Smart Card PKI Architectures

Using the F5 BIG-IP Local Traffic Manager to support federation of cross-domain service access in a Smart Card PKI-enabled architecture.

by Lori MacVittie

Technical Marketing Manager, Application Services



Contents

Introduction	3
Constrained Delegation Model	4
Order of Operations	5
How it Works	6
Conclusion	8
References	9



Introduction

Kerberos has long been considered to reside at the top of the network authentication protocol tree as the most secure and, unfortunately, most complex authentication system. This comes not from the way in which Kerberos is designed, but rather from the complexity of the systems that have grown up around Kerberos that support identity management, especially when applied across organizational boundaries.

The introduction of smart cards as a means to address the inherent weaknesses in password-based identity management architectures has provided for stronger security in organizations adopting such tactics. However, it has also created additional challenges in implementing secure architectures relying on Kerberos for authentication. One of the negative effects of smart cards on organizations was the inability to leverage the functions of an Application Delivery Controller (ADC) in the infrastructure because the ADC was unable to obtain a ticket for services on behalf of the client.

Kerberos delegation, as specified by version 5 of the protocol, resolved this through two new extensions to the authentication protocol: Protocol transition and constrained delegation. Protocol transition allows a service using Kerberos for authentication to obtain a Kerberos service ticket to itself on behalf of a user or proxy without requiring the user or proxy to be part of the Kerberos environment. This is an important feature as it allows users to send a request to a service using credentials that are not acceptable for Kerberos authentication such as a smart card, which presents a client certificate as credentials. This method creates a user token for authenticated users, which is used by a service with the necessary impersonation privileges to ultimately obtain a service ticket for the desired services. The constrained delegation extension allows a service to obtain service tickets restricted to a list of specific services on the network once it has been presented with the appropriate service ticket, which may have been obtained through protocol transition. Constrained delegation is a security-limited version of native delegation as it allows administrators the ability to restrict delegates to a specific set of services.

This model also resolves the issue raised by the federation of domains across organizational boundaries, both external and internal. This capability is achieved through the implementation of Kerberos Protocol Transition (KPT). KPT works across a forest of domains as long as there exists a full transitive trust between all participating domains. The integration of domains across these boundaries is inherently complex and scales poorly, and in some cases is not permitted due to



security reasons. Thus it had previously been the case that users whose identities are not authenticated to a domain controller through which tickets to the desired service can be issued cannot access those services. Previous solutions to this dilemma have been to deploy proxy authentication tiers, which are costly to manage due to the manual nature of mapping user identities to domain identities, and do not scale well in use.

Supporting smart card PKI and federated access without exorbitant costs and additional tiers of infrastructure can now be achieved by leveraging a constrained delegation model and Kerberos Protocol Transition support using the F5 BIG-IP® Local Traffic Manager™ (LTM) with the F5 Advanced Client Authentication (ACA) module.

Constrained Delegation Model

Microsoft has created a Kerberos v5 extension called S4U (Services for Users) that comprises two parts:

S4U2Self - Allows a service to obtain a service ticket to itself on behalf of a client. This is usually used with a client certificates. S4U2Self is *the* Kerberos Protocol Transition extension

S4U2Proxy - Allows a service to obtain service tickets to arbitrary services on behalf of the user with only the user's service ticket to itself. The services are constrained by the administrator. S4U2Proxy is *the* Kerberos Constrained Delegation extension.

Leveraging Kerberos Protocol Transition, client machines do not need to be in the domain and can use any browser; they are not restricted to using Internet Explorer®. This is possible because the intermediary providing access to the services in the domain proxies the requests for the client. The beauty of Kerberos Protocol Transition is that passwords are no longer required, which allows for the use of smart cards for client authentication. The intermediary as a member of the domain, transitions the client request from a non-Kerberos model (smart cards and client certificates) to the required Kerberos model (username, domain membership. It is then possible to access—if authorized—services across domains regardless of the client type and mode of authentication.

In addition, the use of a constrained delegation model in conjunction with a protocol transition implementation eliminates the need for application-specific



passwords, as identity is proven and services subsequently authenticated based on credentials stored within a client certificate or smart card.

This type of delegation is preferable in an environment in which an ADC—or other intermediary interacting with Kerberos-based infrastructures—is leveraged. Kerberos Protocol Transition has added benefits in its ability to more easily support federation of cross-domain users and services, as the mapping of user credentials occurs only at the intermediary and does not require one-to-one mappings of every domain to every other domain.

Not only does this solution significantly reduce the costs associated with deploying an infrastructure capable of supporting smart card users across multiple domains, but it can also scale up the Active Directory infrastructure while unifying the environment. This unification simplifies auditing and change control, which translates into operational efficiencies that reduce both time and budgetary expenditures.

Order of Operations

The introduction of a PKI-based authentication infrastructure can be problematic for architectures relying upon an ADC for load balancing and SSL offload. This is due to the way in which the ADC interacts with the services and security infrastructure, as an intermediary that essentially becomes the “client” in the “client-server” architecture used to implement Kerberos-based infrastructures. In such scenarios, the ADC does not have access to the client’s certificate used to authenticate against an Active Directory Kerberos service, so it cannot be authorized to automatically access applications it manages via expected mechanisms.

When the BIG-IP LTM with ACA is configured to support Kerberos, it acts on behalf of the client, essentially becoming the authenticated client for services. This is accomplished by taking advantage of Microsoft’s Kerberos extension, S4U¹ (Services for Users).

Figure 1 on the following page shows the logical flow of the constrained delegation model.

¹<http://msdn.microsoft.com/en-us/magazine/cc188757.aspx>

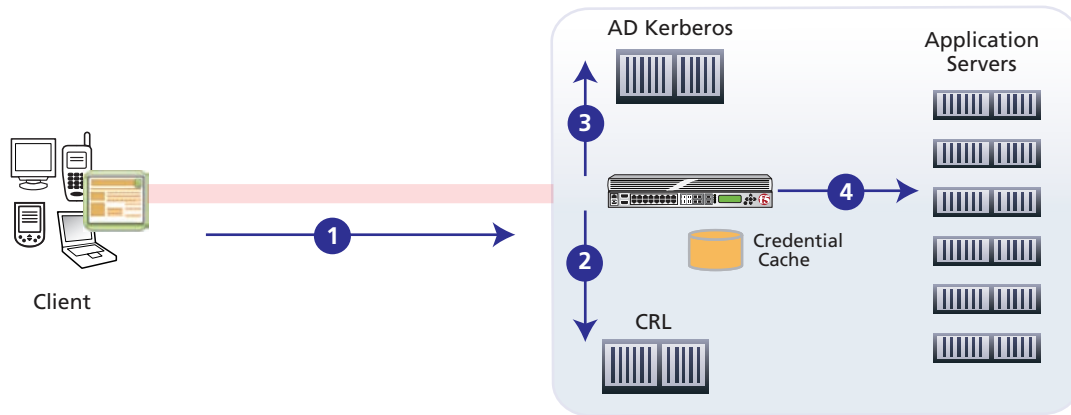


Figure 1: Logical flow of the Kerberos protocol transition and constrained delegation model

1. The client attempts to access service using a SSL client certificate or smart card credentials.
2. The BIG-IP system verifies the credentials are still valid.
3. The BIG-IP system obtains a service ticket for the user (S4U2Self). It also obtains a service ticket for configured back-end server (S4UProxy).
4. The BIG-IP system forwards the user's service ticket to the desired service.

How it Works

In constrained delegation architectures, a virtual server on the BIG-IP system - acting as a Kerberos service principal - joins a Kerberos (Active Directory) realm. The user connects to a BIG-IP HTTPS virtual IP address requiring a client certificate. The client certificate is accepted and verified against the appropriate security mechanisms. The client certificate is then mapped to a user name based on the Subject Alternative Name: User Principal Name field.

The BIG-IP system then uses the S4U2Self Kerberos protocol extension to fetch a service ticket for the user from the KDC (Key Distribution Center). The initial ticket is used to retrieve another service ticket to a constrained service such as Microsoft Outlook® Web Access or SharePoint®. This ticket is encoded into a one-time GSS (General Security Services API, which Microsoft calls the SSPI) token, base64-encoded in the "WWW-Authenticate: Negotiate" request header and passed onto the service.



Both tickets are stored in a credential cache on disk on the BIG-IP system. An encrypted cookie is inserted into the response with a unique pointer to the file-based credential cache. When the user revisits the site, the cookie is decrypted and the credential cache is consulted to generate a new onetime token that is used to authenticate the user to the desired service.

Each subsequent request must have a new confounder in the token, which means a single token cannot be reused. Each request requires that a new GSS token be generated from the cache, although only the first generation requires invocation of external KDC services.

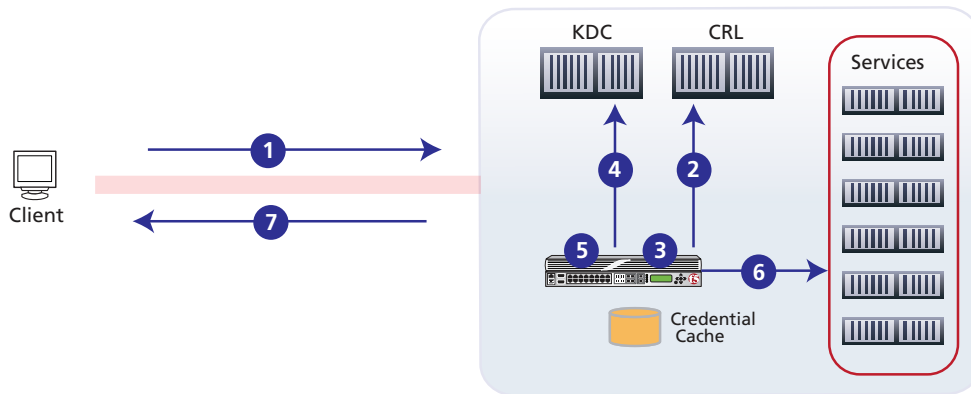


Figure 2: Step-by-step flow of authentication on the first request made by a user in a Kerberos constrained delegation architecture.

1. A request for a service is made via an SSL-enabled connection to the BIG-IP system. An iRule intercepts the client certificate.
2. The ACA module verifies the client certificate is valid.
3. The ACA module extracts Service Principal Name.
4. The User Principal Name and a service ticket to the BIG-IP system are passed to the KDC. The user's service ticket is returned to the BIG-IP (S4U2Self).
5. The service ticket is placed in a credential cache file.
6. The service ticket is encoded and then sent to the requested service in the HTTP headers.
7. Along with the response from the service, a cookie with the encrypted credential cache name is returned to the client.



On subsequent requests the cookie is examined and if it contains valid credentials then those credentials are retrieved from the cache and used again as an authentication header to the service. If no valid credentials exist, the request is treated as if it were a first time request.

Conclusion

The integration of smart card PKI with Kerberos has introduced multiple challenges in scaling authentication infrastructure as well as technical issues involving the use of application delivery controllers. F5 BIG-IP Local Traffic Manager with Advanced Client Authentication is a manageable solution to the problems of federating access to services across multiple domains as well as ensuring that smart card PKI access to services can be utilized regardless of the client's choice of web-browser. Because BIG-IP LTM with ACA acts as an authentication proxy for services requiring Kerberos-based authentication and can intercept client requests, it can map client certificate credentials to Kerberos efficiently without requiring changes to the client and eliminates the need for multiple proxy authentication tiers.

F5 BIG-IP LTM with ACA in Kerberos protocol transition and constrained delegation architectures allows for a more scalable, efficient and secure infrastructure capable of federating access to services across domains and authentication realms, ultimately decreasing the capital and operational expenditures required to keep applications secure, fast, and available.

Technical Brief

Kerberos Constrained Delegation and Protocol Transition in Smart Card PKI Architectures

References

- “Windows 2003 Kerberos Extensions”:
<http://technet.microsoft.com/en-us/library/cc738207%28WS.10%29.aspx>
- “Windows 2003 Kerberos Extensions”:
<http://technet.microsoft.com/en-us/library/cc738207%28WS.10%29.aspx>
- “How the Kerberos Version 5 Authentication Protocol Works”:
<http://technet.microsoft.com/en-us/library/cc772815%28WS.10%29.aspx>
- “Kerberos Constrained Delegation in ISA 2006”:
<http://technet.microsoft.com/en-us/library/bb794858.aspx>
- “Kerberos Constrained Delegation in ISA 2006”:
<http://technet.microsoft.com/en-us/library/bb794858.aspx>
- “Protocol Transition with Constrained Delegation Technical Supplement”:
<http://msdn.microsoft.com/en-us/library/ff650469.aspx>

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

