Direct Certificate Discovery Background

This site only contains limited information on DIRECT -- to learn more, dig into the DIRECT Project wiki.

Introduction

The Direct Project developed implementation guidance with the intent of promoting both flexibility for hosting certificates while also enforcing interoperability for certificate discovery. The resultant guidance arrived at a hybrid approach using DNS and LDAP.

In summary, the approach for Direct Project certificate discovery is:

DNS is used as the entry point leveraging its global discoverability. LDAP is used when the DNS record does not support the CERT record or when LDAP is preferred by the publisher.

Details

System as Certificate Host

A system can choose to store their certificates in any of the following four options:

1) Address-bound DNS CERT Resource Record

2) Domain-bound DNS CERT Resource Record

3) Address-bound entry in an LDAP Server

4) Domain-bound entry in an LDAP Server

The implementation guidance explains in more detail what the CERT records and LDAP entries must look like.

The Direct Certificate Discovery Tool searches for a certificate for the Direct address using the test case that is chosen by the user. Each test case uses a different search query, but all searches are based on the specifications. For example, if the user chooses a hosting test case to look for an address-bound certificate stored in an LDAP server (DTS 556 in v2.0, v2.1.2 or H3 in v3.0), the Testing Tool first searches the DNS for the appropriate SRV records, evaluates them based on their priority and weight, searches the resultant LDAP instance for a "mail" attribute equal to the Direct Address, and returns a certificate if one is found.

The following diagram shows the high-level interaction between the testing tool and the certificate host. Behind the scenes, however, there could be several queries (in the case of an LDAP query).

> *blocked URL*

Diagram of interaction between Testing Tool and SUT when SUT is certificate host.

System as Certificate Discoverer

Each Direct Implementation MUST be able to discover certificates stored in any of the above four configurations. The test cases provided by the tool test that a System is able to discover certificates in all four of the possible hosting configurations.

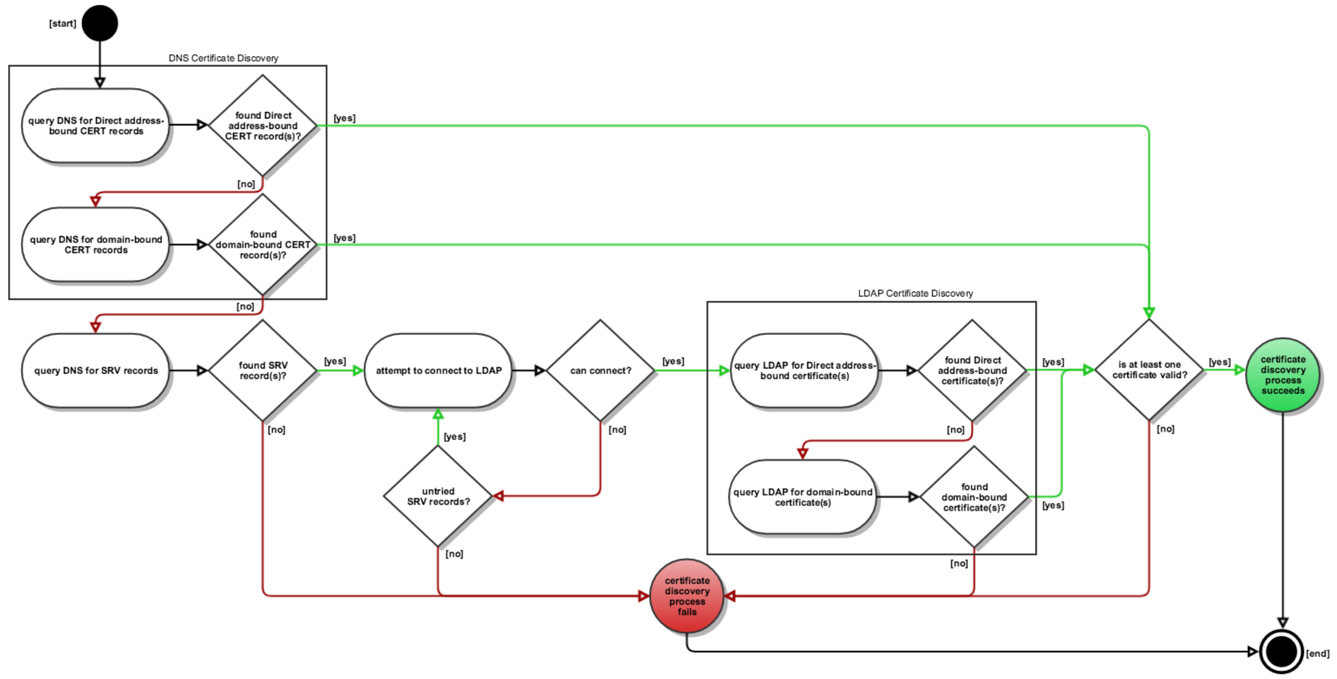
The following diagram shows the interaction between the System and the test tool where the System is the certificate discoverer.

> *blocked URL*

These diagrams show how the tool uses background test data to confirm that the System under test adequately progresses through the algorithm and chooses the correct target certificate.

Direct Certificate Discovery Process

This diagram represents DCDT's understanding of how the Direct Certificate Discovery Process works. You can cross-reference this with our test data here , which provides more details regarding the Discovery testcases and their associated background certificates.


[start]
DNS Certificate Discovery
query DNS for Direct address-bound CERT records
found Direct address-bound CERT record(s)?
[yes]
[no]
query DNS for domain-bound CERT records
found domain-bound CERT record(s)?
[yes]
[no]
query DNS for SRV records
found SRV record(s)?
[yes]
[no]
attempt to connect to LDAP
can connect?
[yes]
[no]
untried SRV records?
[yes]
[no]
LDAP Certificate Discovery
query LDAP for Direct address-bound certificate(s)
found Direct address-bound certificate(s)?
[yes]
[no]
query LDAP for domain-bound certificate(s)
found domain-bound certificate(s)?
[yes]
[no]
is at least one certificate valid?
[yes]
[no]
certificate discovery process succeeds
certificate discovery process fails
[end]

blocked URL

Underlying Specifications

The following diagram shows how the top-level specification, the implementation guidance developed by the DIRECT Project, pulls in different underlying specifications:

> *blocked URL*